PromethEUs

June 2023

PromethEUs’ Joint Publication on EU Data Strategy

The EU’s Data Strategy from a multifaceted perspective. Views from Southern Europe

The PromethEUs network of think tanks, consisting of Elcano Royal Institute (Spain), I-Com – the Institute for Competitiveness (Italy), IOBE – the Foundation for Economic and Industrial Research (Greece) and the Institute of Public Policy – Lisbon (Portugal) has carried out a joint paper on the EU Data Strategy as the main output of its activity in the first semester 2023.

Aiming to contribute to the debate around the Strategy from a Southern European perspective, the paper sets the discussion on the strategy, that the network analysed in three key aspects - economic, geopolitical, and regulatory - with specific applications in key important industries such as healthcare.

EXECUTIVE SUMMARY

Chapter 1: European Data Strategy: Regulatory & Policy Aspects

The chapter describes the EU Data Strategy and some of its most important Acts and Directives, points to their interactions with other legal instruments, and discusses its political, economic and regulatory impacts and risks.

The EU Data Strategy provides the outlines for a regulatory framework that ensures that data can flow within the EU and across sectors, maximizing their potential for innovation. It serves as the political backdrop to recently adopted legal instruments such as the Data Governance Act (DGA), the Data Act (DA), the DSA package, and the Open Data Directive, among others now in development. **The core principle of the EU Data Strategy is to create a human-centred, data-driven, and prosperous economy in the EU.** Contrary to the US or China, this vision does not leave the framework to be defined either solely by market forces or by central-state authorities. **Citizens and SMEs will have a crucial role in the creation and usage of data in the markets.**

The DGA creates new bodies and responsibilities in the data economy, such as data intermediation services, data altruistic organizations or the European Data Innovation Board, in order to establish a trustworthy sectoral or cross-sectoral data sharing infrastructure. It also increases the reach of previous initiatives, such as the Open Data Directive, for the publication of confidential publicly held data. Complementarily, **the DA defines who can use and access what data for which purposes across different economic sectors in the EU**. The dispositions of the DA apply to data holders, citizens and third parties’ usage rights. **Both acts will apply without prejudice to other relevant EU**

law, mainly the GDPR, but also the DMA and the DSA, though there are some grey zones and outright changes, as with respect to the Database Directive.

To further boost the data-driven economy, **the EU Data Strategy envisages the creation of two types of data domains: high-value datasets and nine common European data spaces.** The former refers to datasets of public authorities on specific topics (energy, finance, health, etc..) of which the reuse by businesses and other organizations is considered particularly valuable for the economy, innovation and efficiency. The latter are created to nurture an informational ecosystem based on the free flow of non-personal data across borders, sectors, between businesses, academia, relevant stakeholders, and the public sector.

On the political side, the Commission and its associated bodies (such as the EDIB, the European Data Innovation Board) **will assume a vital role in the coordination of the data-driven economy proposed by the Data Strategy**, as well as a strengthened role in the international representation of the EU. The EU Data Strategy also promotes increasing transparency in the activities of public authorities, enshrined in the DGA and the Public Administration Data Space. Finally, several regulatory acts stress the relevance of international agreements and minimum levels of data protection in third countries, which again sets the stage for the Commission's role in EU representation in the future. Similar to the GDPR, the EU Data Strategy and its associated legal developments may influence the rest of the world concerning rules for sharing and using data.

Regarding its economic dimension, the EU Data Strategy is expected to have a positive, direct and horizontal impact on markets by allowing the reuse of data within and across sectors. The DGA and DA are meant to nurture trust for B2B data sharing but do not actually change the underlying business model or incentives for sharing. Are there reasons for concern regarding the incentives for competitors to share data? Will there be freeriding? Additionally, the DA's anti-competition clauses, its restricted scope concerning types of data, and the possible bypassing of crucial dispositions by gatekeepers may also limit their impact.

SMEs will gain some protection and will face lower barriers, e.g., via fair contractual terms for data access and switching of cloud providers. They are also exempted from some data compliance obligations. However, are these safeguards enough?

From a regulatory perspective, the EU Data Strategy attempts to integrate value chains across sectors and Member-States. This integration process, plus the creation of multiple "competent bodies", will lead to the rebalancing of the *status quo* of the regulatory bodies inside the Member States with possible overlaps in different areas. Will EU Member-States create new regulatory entities or just new responsibilities for the existing ones, and how complex will the resulting network of regulations and regulators be? Will the outcomes be similar between Member States? The provisions of the DGA and the DA also require further investment in human resources and regulatory budgets, which again will reinforce the rebalancing of the regulatory bodies and public administrations in the Member States.

Some of these points are being addressed in the trilogue negotiations following the amendments proposed by the European Parliament and by the European Council in March 2023, but others, such as the lack of incentives to actually make use of the framework and the issue of institutional harmonization, point to a strong need for further coordination at industry and European level.

Chapter 2: Geopolitical aspects of the EU Data Strategy

Data is one of the most valuable resources in today's global competition – but it is not yet seen as a global common that leads to collaboration. So far, global data flows are still governed through a maze of multilateral, bilateral, unilateral, and ad hoc rules, principles, and voluntary frameworks that are not always accepted or applied by all actors. Cross-border international collaboration on this issue is far limited, with ups and downs in the success of a common global agenda on data governance. Also, data governance is getting balkanized in blocs that propose different, if not contrasting, data models. Doing so is as important as strategic for the maintenance of an international security and peace order which growingly relies on the power over data and has strong impacts on three layers: security, economic, and rights.

The European Union's Data Strategy aims to make the EU a leader in a data-driven society. The goal of creating a single market for data is to allow data to flow freely within the EU and across sectors for the benefit of businesses, researchers, and public administrations. **However, the Data Strategy has much to do with the current debate over strategic autonomy -or digital sovereignty- and the way the EU needs to promote its global vision on technology through three lens: security, economy, and rights.**

It is by no chance that the EU has been addressing how their goods, services, assets, and personal data relate to third countries through several ways.

The first approach is regulation, which has been closely followed by most stakeholders. The EU General Data Protection Regulation (GDPR) -the backbone of the EU Data Strategy- only permits the transfer of personal data to those jurisdictions that comply with a sufficient level of data protection through data adequacy provisions. The final texts of both the DSA and the DMA were a thermometer of how the EU aimed to tackle its relationship with actors from third countries. While the major impact of these rules is on the internal single market, the reality is that it addresses many aspects of digital sovereignty -capabilities of states, respect to human rights, and economic leadership.

However, the main challenge for the EU to deploy this regulatory tool as a geopolitical asset relies on whether the EU will get to influence other countries to follow the same approach. It is not only about imposing certain rules to those that already do interact with the EU, but about encouraging others to do the same with their owns. Another challenge for the geopolitical instrumentalization of these regulations is to understand that geopolitical strategies should vary depending on the country and type of technology company, as firms may have different geopolitical approaches.

The Data Act aims to influence the way the EU harness its strategic autonomy or digital sovereignty with third countries and actors. Two critical points exist on this matter. How to define Intellectual Property: since the definition of "trade secret" cannot be changed because it is closed, the Parliament decided to focus on the definition of "data". And how to manage defense-related data which has been excluded because it raised concerns over the potential weaponization of the Data Act by certain companies from third countries. Similarly, the EU should carry out a risk assessment on the weaponization of data to affect EU priorities, interests and vision based on the three primary streams of data that are available for harvesting: user-generated content, information purchased from Original Data Suppliers (ODS), and third-party data services from intermediaries. Likewise, the case of the EU-US transatlantic framework is paradigmatic.

The second approach is the role of multilateral initiatives, "coalitions of the willing" and international meetings. These meetings may be divided in two types: institutionalized organizations and spaces with long-lasting history, and ad hoc, recent coalitions which are aimed at pushing forward specific, tailored topics, and with expected deliverables.

Some examples are the G7 Meeting on Digital and Tech Ministers, and alliances with like-minded countries on a bilateral or multilateral basis, such as Quadrilateral Security Dialogue or Quad, the Digital Economy Partnership Agreement or DEPA, D-10, Tech-10, T-12, among others. In all cases, data has been addressed through several lens: data privacy, cross-border flows of industrial, non-personal data (which impinges on the core of critical infrastructure, critical technologies, and economic security instruments such as export controls and Foreign Direct Investment), how to foster R&D and joint consortiums across countries with sensitive or critical data, or the impact of data usage on fundamental rights.

In the case of the EU, the Union has participated in several initiatives, particularly the G7 and G20. Some initiatives have been particularly critical for the geopolitics of data. In 2019, the then-Prime Minister Abe Shinzo from Japan proposed, during its Presidency of the G20, the Data Free Flows with Trust (DFFT) approach to guarantee the enhancement of cross-border data flows, based on the combination of privacy and security of personal and sensitive data. This is why the EU has an opportunity to partner with Japan and engage closely with the Indo-Pacific region.

The third approach is the building-up of EU technology diplomacy in three main forms. First, by strengthening the number and scope of technical assistance projects in third countries -mostly through the Directorate General of International Partnerships, which was before the development cooperation branch of the European Commission. **Second, by launching a number of regional initiatives with specific partners, focused on digitalization. Third, by setting up the first-ever framework on Digital Diplomacy in 2022.**

A key challenge for the EU is how to partner with developing countries or, particularly, digitally non-aligned countries. Also, all digital diplomacy branches should pay attention to certain technologies that are still underdeveloped, not too marketized or not in place, but that could generate major competition across countries. For example, a Chinese state-owned think tank flagged national security risks of metaverse -which is fed by personal and non-personal data, considering potential political and social issues.

The European Union is developing an increasing package to address the governance of data globally speaking. To do so effectively, it will need to face a number of challenges -from the perspectives of security, economy, and rights- that are not always framed under the existing policies. New scope, intensities, stakeholders' engagement and a higher level of ambition and monitoring will be the drivers to make the EU's leverage of its Data Strategy worldwide successfully with partners.

Chapter 3: The economic impact of Data-Driven Innovation in Europe

The chapter aims to describe the data economy and data industry in Europe from an economic point of view.

Data analytics have opened up a world of opportunities for organizations that can leverage information to tailor their business to market demand. For this reason, more and more organizations are recognizing the value of data and are working towards its efficient and effective management, increasingly consolidating themselves in data-driven business models. Given the importance that data is assuming, its management is one of the keys to technological supremacy. For this reason, it is important to analyse **how the EU is positioning itself in this field compared to other large economies such as the USA and China**.

According to what emerges from the latest version of the report "European DATA Market Study 2021–2023" prepared by IDC, **the US continues to be the dominant player in the global data economy**. The US data market value in 2022 stood at €289.5 billion, nearly four times that of the EU (€73 bn) and more than seven times that of China (€40 bn). The EU occupies second position in terms of size and strength of the data market and data economy if compared against the present international background. **Despite its second position in absolute size, Europe ranks lower than China in terms of percentage change** (+12.6% between 2021 and 2022). China experienced a significant growth in this market, reporting a positive change of 24.1%.

Among the European countries, in 2022 Germany had the largest data market with a value of € 20,351 million (+13.1% on 2021). France and Italy followed, with a data market value of € 12,300 million (+14%) and € 6,886 million (+12.2%), respectively. **The top five Member States (Germany, France, Italy, the Netherlands and Spain) accounted for more than 68% of the EU data market**.

The positive trend in the data market growth is also reflected by the GDP impact. **The country with the largest data economy impact on GDP by 2030, according to the estimates, will be Estonia (12.6%)**, followed by Cyprus and the Netherlands (10.2% and 8.5%, respectively), whereas Greece will remain the least affected country (1.9%). Instead, in Portugal the share of data economy on GDP will be 5.7%, while in Spain and Italy it will be 5.3% and 5.2%, respectively.

However, **the lack of adequate skills risks becoming an important barrier** to data industry development and the adoption of data-driven innovation in the European Union. According to the IDC study, the skills gap for data professionals is growing rapidly, and will expand even greater in the 2022–2025 period. Therefore, there continues to be an imbalance between the supply and demand of data skills in Europe. In France, Italy, Spain and Poland, the number of unfilled positions is expected to climb by 2030 to 6.5%, 6.4%, 4.3% and 3.7%, respectively. Only in Germany is the skill gap expected to decline, from 6.7% in 2022 to 6.4% in 2030.

With the aim of measuring the performance of European countries in the implementation of data driven innovation, I-Com developed **a synthetic index that takes into account 6 variables related to the data economy in Member States**. The variables are: share of data supplier companies out of total number of companies by each country; share of data user companies out of total number of companies by each country; share of data professionals out of total employment; share of data market; share of enterprises analyzing big data internally from any data source or externally out of total enterprises; share of enterprises using cloud computing services out of total enterprises).

On the top of the rankings is Denmark with a score of 100, followed by Sweden, the Netherlands and Finland with scores of 91, 91, 90 respectively. These countries, despite being small in terms of size compared to others, show a good "data ecosystem" and have enterprises that perform particularly well in terms of Big Data and the use of enabling technologies such as cloud computing.

At the bottom of the ranking, we find the countries of Eastern Europe (Romania, Bulgaria, Hungary) and Spain, where the paradigm of data driven innovation looks still little implemented.

Looking at the results, Southern European countries not only need to invest more in skills but also in the development of enabling technologies.

Data management is becoming a crucial development factor for organizations, and SMEs are no exception. Unfortunately, however, **SME companies are often not equipped with an adequate set of skills to exploit the important opportunities that can arise from data analysis**. This factor is inevitably reflected in the ability of small and medium-sized companies to seize the business opportunities related to the exploitation of data. Big data usage figures show that just 11.1% of EU companies with 10 to 49 employees and 18.6% of those with 50 to 250 employees analyze their data internally. Despite this, the share of companies that use external data analysis services is even lower. Adding up the percentages, we see that **only 13.9% of companies with 10 to 50 employees and 23.6% of those between 50 and 250 use big data in some way**. Therefore, from these figures it is evident that most SMEs not only do not collect and analyze data internally but also do not use it at all. Consequently, there is a real risk that the lack of skills in SMEs affects not only the ability to analyze data, but also the ability to understand the importance that such data might have on business performance.

Chapter 4: Digital revolution and the health sector focusing on the Southern European countries

The European Health Data Space (EHDS) planning could enhance the citizens digital access to their private health information, support access of medical professionals to health data, assist academia, regulatory activity and policy making by providing non-identifiable health data while facilitating complete adherence to the strict data privacy standards set by the EU **A variety of benefits is expected since improved access and transfer of health data in the healthcare sector could save 5.5 billion € for the EU over ten years in combination with € 5.4 billion that could be saved for the EU from optimal use of health data by the research and innovation community and also by the policymakers.** Furthermore, **the potential growth of digital health care is estimated between 20-30%. Another critical benefit is the boost of investments in Research and Development (R&D) by facilitating access to Real World Evidence.**

Though the benefits of the EHDS could be significant for healthcare policy and innovation, **certain challenges also emerge.** Health information is the most sensitive type of data, and privacy ensuring should always be a top priority. Therefore, **cybersecurity, storage and connection with other**

information are issues of great concern since the EHDS requires interoperability among many different data sources. Unidentified provision of data for research and other policy issues should also be a critical aspect to ensure. Transparency in data management, privacy protection and taking patient consent could increase trust and foster health digitalisation.

We analyse the digital readiness of the four examined countries focusing on the health sector. We present evidence regarding their performance in the Digital Economy and Society Index (DESI) and its subdimensions, the digital health market projections, and the digital health performance of the country using indexes available from Future Proofing Healthcare Index. Also, we utilise the findings of the report published by the Open Data Institute (ODI) in 2021 (Boyd et al., 2021) to evaluate the performance and readiness at the policy level of Italy, Portugal, Spain and Greece on the six best practice categories, including infrastructure, capabilities development, healthcare innovation, equity, ethics, and public engagement.

Spain is leading among the examined countries in the digitalization and the relative readiness to transform digital health sector. Spain's digital progress is evident since the country ranks 7th in the 2022 DESI index (11th in 2021). Spain leads the way in the connectivity dimension since was in third positions for two consecutive years. The country dynamically promotes new digital services, among others, in the health sector. There is a specific Digital Health Strategy will be developed in the country for the 2021 – 2026 period. It aims to facilitate an environment where the public sector's digital health transformation efforts could flourish by interacting with all stakeholders involved, and it provides governance and monitoring mechanisms. Boyd et. al. (2021) indicate that the policy stage at Spain is vaguer, since there is not relative specified strategy regarding the secondary use of health data. The main challenges that country has to face to facilitate the policy environment are the slow and stalled implementations of the relative efforts and the potential fragmentation since the secondary use of health data is in regional level.

The 15th position in the 2022 DESI index is allocated to Portugal showing a relative progress compared to the previous year (16th). In the field of e-health, Portugal's environment is quietly advanced since the country has implemented two consecutive relevant strategies, the ENESIS 2020 (ran until December 2019) and the ENESIS 2022. The goal of the renewed strategy was to establish the framework and conditions for the various stakeholders of the health system to contribute to its evolution. A representative example is the 'From Big Data to smart data: putting data to work for the public's health' which is the strategy of the Portuguese National Health Service. Challenges, as identified by Boyd et. al. (2021), include the potential for fragmentation, the early implementation stage, the lack of ecosystem capability and the limited patient and multi-stakeholder participation.

Italy, the third major EU economy, **is placed three positions after Portugal (18th) among the EU countries in 2022.** The 25.1% (€ 48 billion) of the Italian Recovery and Resilience Plan (RRP) (€ 191.5 billion) aims to foster digital transition. Throughout the RRP € 1.3 billion is invested to transform the electronic health records, ensuring interoperability and portability in regional level. To proceed with the first payment request, Italy accomplished 51 milestones and targets. One of them, worthy of mentioning in the context of this report, is the 'Sanità connessa' (Connected Healthcare facilities). The purpose of 'Sanità Connessa' is the establishment of symmetric connectivity (1 Gbps - 10 Gbps subject to facility type) among 12,300 healthcare facilities. Top policy challenges include increased fragmentation, data quality and the strictness of interpretation of local data privacy laws regarding the secondary usage of health data (Boyd et. al, 2021).

From the examined countries Greece ranks last in the 25th place, in spite of the recent progress. The RRP of Greece allocates a significant part (more than € 2.7 billion) towards digitalisation of public administration, where public health digitalisation is also included (European Commission, 2022a). Key investments include the "Planning Unification and support of the Operation of the Registries of IDIKA S.A. in the Field of Health and Social Security" and the "Digitalization of the archives of the Public Health System" account for € 15.2 and € 117.8 million respectively (Greek Government, 2021). According to the Boyd et al. (2021), the main policy challenges for Greece include the lack of clarity regarding the implementation strategy of the health data usage The Bible of Digital Transformation by the Digital Governance Ministry facilitate, to some extent, the secondary use of healthcare data.

There is a need to for a unified roadmap for the proper utilization of data that could support transformation/rationalization of health care, health spending and the promotion of clinical research and innovation. Establish precise rules and policies for data security and privacy in the healthcare industry is imperative. Encourage standardisation procedures, which could entail the adoption of standard terminology and processes by various healthcare stakeholders, could also be useful. Effective quality assurance mechanisms could contribute significantly to the task. Transparency in data management, privacy protection and taking patient consent could increase trust and foster health digitalisation. Last, but not least, fostering cooperation and collaborations amongst various healthcare stakeholders could significantly promote the digitalisation of healthcare and the successful secondary data usage.

CONTRIBUTORS

Chapter 1: European Data Strategy: Regulatory & Policy Aspects

IPP, Institute of Public Policy
Steffen Hoernig, André Ilharco

Chapter 2: Geopolitical aspects of the EU Data Strategy

Elcano Royal Institute
Raquel Jorge Ricart

Chapter 3: The economic impact of data-driven Innovation in Europe

I-Com, Institute for Competitiveness
Stefano da Empoli, Maria Rosaria Della Porta, Lorenzo Principali, Domenico Salerno

Chapter 4: Digital revolution and the health sector focusing on the Southern European countries

IOBE, Foundation for Economics & Industrial Research
Aggelos Tsakanikas, Alexandros Moustakas, Maria Theano Tagaraki

Table of contents

Chapter 1: European Data Strategy: Regulatory & Policy Aspects

1.1 Overview and purpose of the European Data Strategy

The EU Data Strategy is based on the Communication issued by the European Commission in 2020.[1] **It is a 5-year plan and strategy that presents a vision of a data-driven economy in the EU and sets the guidelines for the future regulatory framework. It will ensure that data can flow within the EU and across sectors,** maximizing its potential for innovation. Secondly, this framework will **mirror European rules and values in its application to fields such as personal and non-personal data protection, consumer protection legislation or competition law.** The strategy adopted by the EU differs from other data markets such as the US and China. Its vision is based on a human-centred economy and society. Thirdly, it will address the rules for access to and use of data - these must be "fair, practical and clear", and transparent and trustworthy data governance mechanisms will be designed. The approach to international data flows shall be open, but assertive, and always based on European values such as fair competition or protection of individuals' rights.

The Data Governance Act (DGA) and the recently proposed Data Act (DA) constitute two significant steps in the implementation of the EU Data Strategy. The DGA instructs Member States and their designated "competent authorities" to maximize their openness regarding the sharing of data held by public entities, even in the case of confidential data. The DGA also outlines the role of and rules for data intermediaries (further on explained) and incentivizes data altruism organizations and practices. On the other hand, the DA is concerned with fairness and autonomy in data markets, especially for the Internet of Things (IoT). It defends users' rights to their data and their (re)use, while it also determines that fair and reasonable access conditions must be provided by data holders on a number of occasions in the presence of market power. While the DGA is focused on the institutional framework for data sharing, namely through the indication of clear responsibilities for the main actors in the data economy, the DA will regulate who can use and access what data and for which purposes in the EU.

Additionally, the 2020 Data Strategy proposes the creation of Common European Data Spaces focused on the sharing and pooling of data across the EU and sectors. These data spaces are expected to cover the nine areas described below. Here, **the Commission establishes that data must be made available according to the FAIR principle (Findable, Accessible, Interoperable and Re-usable),** which follows the spirit both of the DGA and the DA.

With the creation of nine European data spaces, these Acts point to the European vision of a data market, based on European principles such as fair competition or an open and non-discriminatory market: A data economy where "undertakings compete on quality of services, and not on the amount of data they control" (EU Data Strategy, May 2022, Recital 2).

[1] COM/2020/66, "Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of The Regions: A European strategy for data". https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1593073685620&uri=CELEX%3A52020DC0066

1.2 Legal Instruments

1.2.1 Data Governance Act: Institutional Framework for data sharing. Intended to create trust that rights and freedoms are respected when data are shared

The DGA came into force on 23 June 2022 and will come into effect on 24 September 2023. It creates a regulatory framework that seeks to promote trust in the European data environment and markets. First, the **DGA sets out a framework for the re-use of publicly held protected data**, without creating any right of access. For example, sensitive data such as those related to national or public security are explicitly excluded. The Open Data Directive of 2019 already mandates the release of public sector data, however, several types of data protected as confidential, intellectual property rights, or personal data not otherwise protected by the GDPR, were not covered by this Directive, which left a significant gap in the "data map" envisaged by the EU Data Strategy. The **DGA prohibits the Member States' public bodies to enter into exclusive data-sharing agreements or concede these rights exclusively to any entity**. The only allowed exception is if "an exclusive right to re-use data (…) [is] necessary for the provision of a service (…) in the general interest that would not otherwise be possible". Competent authorities, nominated under the DGA and in charge of supervising the implementation, are entitled to impose other conditions on the terms of re-use, making sure they are non-discriminatory, proportionate, objectively justified and that they do not restrict competition.

Second, the DGA defines **data intermediation services providers (DISPs)** as providing "a service which aims to establish commercial relationships for the purposes of data sharing between an undetermined number of data subjects and data holders on the one hand and data users on the other …". According to the Commission, **these entities will be essential to assure fair competition and the availability of data across countries and sectors**, especially for start-ups and SMEs. The Commission proposes a control mechanism for DISPs, based on mandatory registration with (although no regulatory approval is required) and ex-post supervision by the competent authorities, including sanctions for misdemeanours, for these entities.

Third, the Data Governance Act presents the concept of "**data altruism organizations**" (DAOs). Data altruism is defined as the "**voluntary sharing of data on the basis of the consent of data subjects to process personal data pertaining to them**, or permissions of data holders to allow the use of their non-personal data without seeking or receiving a reward that goes beyond compensation related to the costs" of sharing their data for objectives of general interest. This definition covers purposes such as healthcare, mobility, provision of public services, official statistics, among others. The Commission will publish a "rulebook" setting out further instructions and information requirements for recognition as DAO and a European Altruism Consent Form for data subjects.

Fourth, the **DGA proposes the establishment of national "competent authorities" and the creation of a European Data Innovation Board (EDIB)**, a technical body composed of experts representing competent authorities along with other European institutions and expert bodies. The main tasks of the EDIB will be to advise and assist the Commission, as well as to propose guidelines for the common European data spaces.

Finally, the **DGA defines some rules about lawful and unlawful transfers of data to third countries**. Any entity receiving data under this Regulation must take all reasonable measures, including contractual arrangements, to prevent the international transfer or governmental access to non-personal data held in the Union where such action would create a conflict with Union or each Member States’ national laws. Third countries’ court or administrative decisions to transfer or give access to non-personal data held in the Union shall be recognised only if based on an international agreement in force between the requesting third country and the Union or the Member State.

1.2.2 Data Act: Creating a fair data economy – Sharing of IoT data

In February 2022, the Commission published its proposal for the DA, regulating who can use and access what data for which purposes across all the economic sectors of the EU. By data, the Commission means “any digital representation of acts, facts or information and any compilation of such acts, facts or information, including in the form of sound, visual or audio-visual recording”.

The type of data targeted by the DA is the data generated by connected devices, be it personal or non-personal data. This means it targets principally products and services connected to the internet of things (IoT).

Directly affected by the new rights and obligations envisioned in the DA are stakeholders such as the producers and manufacturers of the connected products and related services, its users, data holders (legal or natural person who has the right/obligation to make certain data available), cloud services providers in the EU, data processing services providers or public bodies that require data holders to provide a specific data in exceptional circumstances. **The DA states responsibilities, duties, rights and obligations for these stakeholders in specific topics such as data access and sharing or the protection of trade secrets and confidential informatio**n.

Regarding data access and sharing, connected products and related services must be made in a way to allow users to access their data easily, and to be informed pre-purchase about the nature and the volume of data likely to be generated by its use. Data holders will be obliged to make the data available to third parties upon user request. Also, trade secrets must be protected when data are shared.

Data holders are entitled to reasonable compensation for making data available to third parties. However, there are exceptions such as the provision of data to public bodies in exceptional circumstances, such as public emergencies, where data must be granted without delay and free of charge.

Finally, the DA seeks to facilitate the switching of business customers between cloud and data processing services[2] and to adapt contract law to “prevent the exploitation of contractual

[2] The proposal for a digital bill unveiled by the French government on May 10th, 2023, includes rules very similar to those in the DA for the switching of cloud providers, with the aim to speed up significantly the protection of both French cloud providers and cloud users (Euractiv 2023, France 2023), as compared to the DA approval timeline.

imbalances that hinder fair data access and use for micro, small or medium-sized enterprises." The latter is part of a set of rules to minimize the regulatory burden on SMEs and protect them from potential abuses by larger market players. Also connected to the protection of SMEs against larger players, the DA typifies situations when contractual terms regarding the access or use of larger companies' data by SMEs are to be considered unfair. Excluding the price to be paid, both contracting parties must be able to influence the negotiations of the terms of the contract.

Since the publication of the initial proposal of the DA by the Commission, both **the European Parliament and the European Council have proposed several amendments to this text**. On March 14th 2023, the European Parliament published its amended version of the DA for the trialogue. In this augmented version, the EP tries to clarify the DA text by providing more details about which kind of data and stakeholders are targeted by each disposition, renames the national competent authorities as "data coordinators", and reinforces provisions on trade secrets protection, among other revisions. The **March 17th version of the Council has common concerns with the EP text**, namely the need to clarify concepts and dispositions and the strengthening of trade secrets protection. This version also includes modifications on the dispositions regarding the interplay between the DA and sectoral and horizontal legislation, such as the GDPR. It also provides clarification on the terms of "reasonable compensation", includes SMEs (under certain circumstances) in the obligation to share their data with public authorities in situations of exceptional need, and includes modifications concerning the freedom of consumers in switching data processing services.

1.2.3 The nine European common data spaces

To reinforce the creation of a data economy in the EU, the **Commission proposed the establishment of thematic data spaces**. These nine data spaces are created to nurture an informational ecosystem based on the free flow of non-personal data across borders and sectors and between businesses, academia, relevant stakeholders, and the public sector. Such data spaces would be:

- **A Industrial (Manufacturing) Data Space**: According to the EU Data Strategy, the potential value of the use of non-personal data in manufacturing at € 1.5 trillion by 2027. This data space will be designed to significantly enhance the competitiveness of European industries. Together with Regulation 2018/1807, the DA is set to determine new dispositions regarding the usage rights of co-generated industrial data (IoT data created in industrial settings).
- **A Green Deal Data Space**: This data space will make available data concerning climate change, circular economy, zero-pollution, biodiversity, deforestation, and compliance assurance. For this, the Commission mentions the revision of older legislation and the "GreenData4All" initiative. Also, in line with the Data Act, the Green Deal Data Space will start collecting, sharing, processing, and analyzing data of reusable data services on a large scale to assist in assuring compliance with environmental legislation.
- **A Mobility Data Space**: This data space will be focused on the processing and availability of the large amounts of data expected to be generated by automobiles (electric or not) on their

movement, maintenance, and reparation. The predicted growth of transport activities in the next decades makes this data space fundamental for topics such as the environment or smart cities. New interconnected platforms will be available to provide data on issues such as road safety, traffic and multi-modal travel information services, generated both by the public and the private sectors.

- **A Health Data Space**: The Health Data Space aims to increase the quality of healthcare while decreasing its costs and fostering innovation. The implementation of EU citizens' rights to re-use and port their personal health data is fragmented within and between the Member States. Health institutions' rules of governance also differ strongly, especially between countries. According to the Commission, the Health Data Space will require the deployment of new legislative and non-legislative measures, data infrastructures and capacities focused on the interoperability and flow of health data across institutions and borders.[3]
- **A Financial Data Space**: EU regulation and the 2015 Payment Services Directive fostered the openness of the financial markets and institutions. The Commission seeks to promote integrated capital markets, improve market transparency, and support sustainable finance in the EU. For this, the Commission promises to explore future additional steps not mentioned in the Data Strategy and to further facilitate access to public disclosures of financial data or supervisory reporting through this data space.
- **An Energy Data Space**: The objective of the Energy Data Space is to facilitate innovative solutions and support the decarbonization of the energy system. For this, the Commission is determined to legally require interoperability and transparent procedures for access to data, as well as to promote interoperability in smart buildings and products, their energy efficiency, improved consumption, and integration of renewable energies.
- **An Agriculture Data Space**: The Commission seeks to go further than the current code of conduct on contractual agreements and common practices in agriculture regarding the sharing and pooling of data. It aims to fulfil the potential impact of data in agriculture through interconnecting the processing of agricultural, machinery, earth observation, meteorological and other types of data. The accessibility of such data in a common data space should promote fair contractual relations and strengthen the capacities for monitoring and implementing common policies while reducing the administrative burden for EU Member States' public authorities.
- **Public Administration Data Spaces**: Data quality in public procurement and its accessibility differ across EU Member States. The public administration data spaces will focus on law and public procurement data, as these are understood to be fundamental to promote transparency and accountability of public spending, fight corruption and improve spending quality. Thus, the Commission proposes to issue a data initiative regarding procurement data, as well as a governance framework. Also, the Data Strategy foresees the provision of guidance on common standards and interoperable frameworks for legal information held at the European and national levels.

[3] In chapter 4 of this policy paper, IOBE describes the Health Data Space in detail.

- **A Skills Data Space**: The data-driven vision for EU economies requires high-quality data on qualifications, learning opportunities, jobs, as well as on the skill sets of people. In this regard, the Commission proposes to support Member States in the development of digital credential transformation plans and in the preparation of re-usable datasets of qualifications and learning opportunities. Also, in collaboration with Member States and key stakeholders, the Commission will implement a governance model for the on-going management of the Europass Digital Credentials Framework.

1.2.4 Open Data Directive: access to data held by public institutions

The **Open Data Directive** (ODD) entered into force on July 16, 2019, and had to be implemented in national regulation by July 17, 2021. **It is the first EU Directive requiring public bodies to make their data open by design and default**. Many of the principles put forward in the DGA and DA can already be found in the ODD.

The ODD states that access to documents must be free of charge by default and will be granted on request. Member States’ public bodies shall take no longer than 20 working days to answer each request. The licenses for the re-use of data will not be subject to conditions unless such conditions are objective, proportionate, non-discriminatory, and justified on grounds of a public interest objective. Also, data obtained in publicly funded research will be opened or remain in an open-access regime.

The Directive presents the notion of “**high-value datasets**” which are defined as “documents the re-use of which is associated with important benefits for society, the environment and the economy, in particular**, because of their suitability for the creation of value-added services**”. According to the ODD, these **high-value datasets must be available free of charge, machine-readable, provided via APIs, and provided as a bulk download, where relevant**. The criteria to classify datasets into “high-value datasets” refer to each dataset’s ability to “generate significant socioeconomic or environmental benefits (…) [,] benefit a high number of users, in particular, SMEs (…)[,] assist in generating revenues (…) [,and] be combined with other datasets”. Among the sectors are geospatial, earth observation and environment, meteorological, statistics, companies and company ownership, and mobility. The Commission was tasked to propose an implementing act specifying the necessary arrangements for these high-value datasets, which is being developed to this day.[4]

The Open Data Directive updates the two previous Directives 2003/98/EC[5] and 2013/37/EU[6]. Taken together, these three Directives gave birth to the Portal www.data.europa.eu. This portal is run by the Publications Office of the EU and currently makes available more than 1.5 million datasets from Member States’ public bodies and other international organizations.

[4] The latest draft of the Commission proposal can be found here: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12111-Open-data-availability-of-public-datasets_en.

[5] https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX%3A32003L0098

[6] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32013L0037

1.3 Interactions with other EU legal instruments

1.3.1 Declaration of Digital Rights of 2022

The **2022 Declaration of Digital Rights** (DDR) is based on the EU Charter of Fundamental Rights and the EU Treatises' principles (adapted to the digital environment) and shines light on many points declared in the DGA and the DA. Contrary to the latter Acts, the **DDR is a recommendation and is not legally binding**. The vision enshrined in this document is focused primarily on putting people at the centre of the digital transformation, promoting safe and secure participation, sustainability, solidarity, and inclusion in the digital space, and guaranteeing individuals' freedom of choice in the presence of powerful algorithms and artificial intelligence services.[7]

Article 1d) of the DDR states that the EU commits to "actively promot[e] this vision of the digital transformation, also in our international relations". **Article 31.2 of the DGA shields any EU organization from being forced by external judicial or administrative decisions to transfer or give access to non-personal data it may hold**. Only based on an international agreement shall this transfer happen. The same is stated in the Article 27 of the DA. This clause binds any requesting third country to the political will of the EU and its Member States and forces it to comply with minimum levels of digital security and data protection if it wants to obtain access.

The DA is a **clear step for the enforcement of Article 17 of the DDR**, "[e]veryone has the right to (…) control (…) how their personal data are used and with whom they are shared". According to the DA, data holders shall "make available to the user (…) data generated by its use of a product" and make this data available to third parties. These DA dispositions match the EU's commitments regarding the privacy of individuals' control over data (Art 17, 18, 19 DDR).

Together with the Open Data Directive, the DGA provides legal support to ensure the enforcement of Article 7b of the DDR regarding digital public services online. Reaching even further concerning the accessibility levels of public data, the DGA helps to guarantee a "wide accessibility and re-use of public sector information".

1.3.2 Digital Markets Act and Digital Services Act

The **EU Data Strategy refers in section 5A that control of data by "Big Tech" will be dealt with in the Digital Services Act package**, consisting of both the Digital Markets and Digital Services Acts (DMA and DSA), while the DGA does not mention either of them.

The Data Act was adopted a few months after the Digital Services Acts package, and thus was designed to work side by side with these two acts. DA recital 10 states that it applies without prejudice to the DSA, and DA recital 36 explicitly mentions the DA's consistency with the DMA. Additionally, Article 5.2 of the DA excludes any entity considered a "gatekeeper" under the DMA as eligible to be considered a third party for data access rights. There is however some uncertainty on

[7] https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733518/EPRS_BRI(2022)733518_EN.pdf

this point, in that the DA concerns the data generated by IoT devices, but not derived or inferred data. Additionally, neither the DA nor the DSA package prevent gatekeepers from buying data holding rights or data holders' companies. This is important since the DA seems to prohibit gatekeepers only to acquire generated data from IoT device manufacturers, which may not be the same entity as data holders[8].

1.3.3 GDPR of 2016, ePrivacy directive of 2002, ePrivacy Regulation (upcoming)

The DGA is applicable without prejudice to legislation such the General Data Protection Regulation (GDPR or Directive 2016/679), implying that public bodies must ensure the respect for the nature of re-used data according to the legal provisions in force and by the use of techniques such as anonymisation, generalisation, and randomisation, among others. If the re-use request cannot be granted due to a lack of formal consent, the public body must make its best efforts to support the requester in obtaining the necessary consent from data subjects.

The DA relies on the rules provided by the GDPR framework regarding the processing of personal data and international data transfers and storage. It assumes a complementary and expansionary nature and under no circumstance shall it be applied or interpreted to restrict or limit rights to personal data, privacy, and confidentiality of communications (Recital 7). Likewise, if the **GDPR grants a user access to the personal data generated by their use of a device**, in the case of a natural person the DA establishes that the "user (…) is further entitled to access all data generated by the product, personal and non-personal" (Recital 30). Also, in situations where the user is not the data subject (enterprises, data traders), the DA mirrors the GDPR's legal requirements, such as the consent of the data subject or legitimate interest.

The proposed ePrivacy Regulation[9] was designed to replace the ePrivacy Directive of 2002. Still under development, the **ePrivacy Regulation seeks to protect the rights of internet users, more specifically the confidentiality of their communications**. This protection shall cover any form of digital communication, from instant messages, emails, metadata, to cookies and IoT. It has many connections to the GDPR and some to the DA. The ePrivacy Regulation will complement GDPR rules on personal data processing by providing specific rules on electronic communications and therefore will take precedence over the latter. As with the DA, the ePrivacy Regulation applies to personal and non-personal data and relies on user consent for the processing of personal data (and the data users generate). However, while the DA gives rights to the users to choose who shall access the data they generate, the ePrivacy Regulation grants individual rights related to the confidentiality of their communications. Furthermore, DA Recital 15 explicitly excludes from its scope many of the ePrivacy-targeted devices: "products that are primarily designed to display or play content, or to record and transmit content, amongst others for the use by an online service should not be covered by this Regulation". Finally, the ePrivacy Regulation requires user consent to usage by any actor of the data (or metadata) they generate while using an electronic communications service, a service

[8] CERRE (2023), Data Act: Towards a balanced EU data regulation, p.18. (www.cerre.eu)

[9] https://eur-lex.europa.eu/legal-content/EN/HIS/?uri=CELEX:52017PC0010.

over an electronic communications network or services or networks that are publicly available. For example, this consent shall be required for sending direct marketing communications to the user.

1.3.4 Proposals for AI Act of April 2021 and AI Liability Directive of September 2022

The EU has approached the regulation of AI through two recent proposals: the Regulation called “AI Act”[10] and the AI Liability Directive[11]. **The proposed AI Act is focused on providing a human-centric, horizontal regulatory framework for the development, placement on the market and use of AI systems in the Union**; being a “Regulation” it will apply directly in each member state. On the other hand, the proposed AI Liability Directive establishes legal responsibilities for the use of AI, and being a Directive each Member State will have to integrate its dispositions in their national legal framework.

The AI Act shares its policy purpose with other instruments such as the EU Data Strategy and the DGA, while connecting more directly with other instruments. For example, it is explicitly complementary to the DA, via the application of the non-discrimination principle as a mandatory requirement to “minimise the risk of algorithmic discrimination, in particular in relation to the design and the quality of datasets used for the development of AI systems” (AI Act, Explanatory Memorandum, p.4).

1.3.5 Proposal for Gigabit Infrastructure Act of February 2023

While the proposed Gigabit Infrastructure Act, Gigabit Recommendation and Consultation[12] themselves do not contain references to the European Data Strategy, the impact assessment of the first indicates that high-quality infrastructure is a necessity for the data economy: “The European Data Strategy adopted in February 2020 foresees that the global data volume will reach 175 zettabytes and the data processing model will change to 80% smart connected objects and 20% centralised computing facilities by 2025. The successful and efficient rollout of highly secured and state-of-the-art fibre and 5G networks is therefore indispensable for future digital services and the industrial data wave.”

1.3.6 Intellectual property rights

The DA does not change the legal status of intellectual property rights and trade secrets, with one exception: **Databases containing data from IoT devices or related services will not fall under the application of the EU Database Directive** (Directive 96/9/EC) to make sure that these databases can

[10] https://eur-lex.europa.eu/procedure/EN/2021_106.
[11] https://eur-lex.europa.eu/procedure/EN/2022_303.
[12] https://digital-strategy.ec.europa.eu/en/news/commission-presents-new-initiatives-gigabit-infrastructure-act-proposal.

be accessed and used under the provisions of the DA. This means that DA databases do not qualify for the *sui generis* right under Database Directive, which will require its review.[13]

Furthermore, **the regime of disclosure of trade secrets may be abused via data transfers under the DA**. Articles 4(3) and 5(8) of the DA state that "[t]rade secrets shall only be disclosed provided that all specific necessary measures are taken to preserve the confidentiality of trade secrets in particular with respect to third parties", and that "to the extent that they are strictly necessary to fulfil the purpose agreed between the user and the third party and all specific necessary measures agreed between the data holder and the third party are taken by the third party to preserve the confidentiality of the trade secret". Article 8(6) of the DA states that unless if provided by other EU or national law or by DA Article 6, "an obligation to make data available to a data recipient shall not oblige the disclosure of trade secrets within the meaning of Directive (EU) 2016/943" (Trade Secrets Directive). It is clear that the definition and prerequisites of "trade secrets" formulated in the latter Directive will be important for the internal coherence of the DA, as under its Article 8(6) data holders may overclassify important data as "trade secrets" to avoid sharing data.

1.4 Effects of the European Data Strategy in Three Dimensions

This section addresses the impact and problems of the European Data Strategy in the light of three dimensions: political, economic, and regulatory. We will address each of these dimensions in turn.

1.4.1 Political Dimension

The goal of the Communication on the EU Data Strategy (COM/2020/66) and subsequent acts is to make the EU "become a leading role model for a society empowered by data to make better decisions – in business and the public sector." (p.1). Politically, there are various dimensions contained in this goal: first, the **EU needs to become more autonomous and a model to other countries and blocks**; second**, EU societies are expected to grow on data-based and data-driven innovation** and on a single market for data with sharing across borders and sectors; third, the two **previous points will be based on EU identity and values**, namely the role and protection of its citizens' individuals rights, and on market-based competition.

The Commission and its bodies (such as the EDIB) will assume a vital role in the coordination of the data-driven economy. It is important to consider how the EDIB will work. According to the DGA, this body will assume the form of an expert group (Article 29). This group will be composed of dozens of representatives of national competent authorities named under the DGA, the Commission and other EU bodies[14], bodies representing SMEs and other bodies in specific sectors or expertise. The Commission will chair the sessions and have the power to appoint individual experts when required. The **role of the EDIB is to advise and assist the Commission to monitor the developments of the**

[13] CERRE (2023, p. 22-24) and European Commission (2022).

[14] The European Data Protection Board, the European Data Protection Supervisor, and the European Union Agency for Cybersecurity (ENISA).

provisions of the DGA. It works as a point of contact between the Commission and important stakeholders involved in the process: national competent authorities and sectoral stakeholders (industry, research, academia, civil society, among several others), and its role is to advise the Commission on the development of a "consistent practice" in domains such as data altruism across the Union (art.30, b)) or help in "developing guidelines" on, for example, how to best protect commercially sensitive non-personal data (art.30, d)) or cybersecurity requirements for the exchange and storage of data (art.30, e)).

The existence of the EDIB guarantees a forum between all the relevant stakeholders which is crucial to the success of the transformation proposed in the EU Data Strategy. However, its constitution itself may not be harmonized enough. For example, the DGA states that competent authorities "should be chosen on the basis of their capacity and expertise" and if questions regarding compliance with the GDPR arise these entities "should seek (…) an opinion or decision of the competent supervisory authority established pursuant to that Regulation" (recitals 44 and 51). Are there different levels of "capacity and expertise" among Member-States? How will the Commission act when facing repeating dissent in the EDIB?

The Commission's coordination role will be fundamental for the openness or closure of EU data to other economic blocks, such as China or the US,[15] and the interaction between EU Member States. This responsibility is clearly stated in the DGA and DA, also, as stated above, by the requirement of international agreements and compliance with minimum levels of data protection for the processing of international data transfers or access to non-personal data held in the EU (DGA recital 22 and article 31; DA Recital 77 and article 27, 2)). Centralizing this coordination should avoid that a divide-and-conquer strategy by outside actors can be successful.

The implementation of the EU Data Strategy will also have **consequences for the equilibrium between institutions within Member States, via the requirement to define competent authorities under the DGA and the DA**. A lack of coordination between the 27 Member States may lead to a heterogeneous institutional framework and *ad hoc* adjustments of relationships between public institutions, or even the merger between regulatory entities. This institutional process may significantly delay the full implementation of the EU Data Strategy. A further issue in this respect is the potential for confusion created by the determination of administrative fines and penalties by individual Member States, for which, so far, no guidelines have been set out.

The EU Data Strategy also promotes increasing transparency in the activities of public authorities, with the DGA extending the reach of the Open Data Directive, stimulating the sharing and openness of publicly held data. The promotion of an open data flow from public authorities is also envisioned in the development of other instruments, such as the Public Administration Data Space or in some of the High-value Datasets under the ODD. Internally to the EU, the existence of more **horizontal data flows may promote coordination between social actors such as economic groups, political parties, or civil society organizations**. The availability of data about EU Member States may also

[15] In May 2023, the European Commission is still analysing the proposed EU-US Data Privacy Framework, with a decision about its "adequacy", clearing the way for free data flows, expected before the summer.

increase local conscience and activism, influencing the governance and policy priorities of cities and urban centres.

1.4.2 Economic Dimension

In the economic dimension, **the European Commission expects the Data Strategy to have a positive, direct, and horizontal impact on markets by allowing the reuse of data across sectors.** In fact, a recent study by the OECD reports that **"data access and sharing is estimated to generate social and economic benefits worth between 0.1% and 1.5% of** gross domestic product **(GDP) in the case of public-sector data, and between 1% and 2.5% of GDP** (in a few studies up to 4% of GDP) **when also including private-sector data"[16].** The Commission estimates that **increasing the availability of data for commercial use** and innovation between businesses and empowering consumers and companies using connected products and related services **can generate up to 196.7 billion euros a year by 2028.[17] The Commission also estimates that the application of the DA dispositions alone will create up to 2.2 million jobs in the period 2024-2028[18].**

One important component of the EU Data Strategy vision is increased competitiveness and the stimulus to invest in research and innovation. The DGA and DA are meant to create trust for B2B data sharing, but do not actually change the underlying business model or incentives for sharing. Voluntary contributions to sectoral data spaces, in the expectation that the other companies will also contribute, is an invitation to freeriding. Thus, some kind of coordination mechanism seems to be necessary to create mutual commitments to share data, which, considering the experience with network sharing agreements in the electronic communications sector, will arouse the suspicions of competition authorities. Either way, more competition based on shared data will only materialise if there are enough incentives to produce the data to be shared in the first place – while sharing may reduce the incentives to do so competitively.

On the other hand, **the DA also contains two propositions that explicitly limit competition of certain types. First,** there is Article 6(2)e that prohibits third parties providing aftermarket services from using a data holder's data to develop a competing product or service. This **provision attempts to strike a balance between the overall speed of innovation and individual incentives, by protecting the latter while allowing for non-competing innovation.** But this comes at the expense of less innovation by third parties. CERRE[19] refer trade secrets, patents, and copyright protection as alternative means to achieve the same aim. **On the other hand**, the DA applies to generated data, not to inferred or derived data, which may maintain the incentives for investment in research and

[16] OECD (2019), "Risks and challenges of data access and sharing", in Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-use across Societies, OECD Publishing, Paris, https://doi.org/10.1787/15c62f9c-en.

[17] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13045-Data-Act-&-amended-rules-on-the-legal-protection-of-databases_en.

[18] European Commission (2022), Study to support an impact assessment for the review of the database directive. https://copenhageneconomics.com/wp-content/uploads/2022/02/study-to-support-an-impact-assessment-for-the-review-of-the-database-directive.pdf

[19] CERRE (2023), Data Act: Towards a balanced EU data regulation. (www.cerre.eu)

innovation. **The core idea here is for companies not to focus their resources and business model on keeping data, but rather to create value from transforming and combining data.** Lastly, this provision is likely to invite litigation about what "competing products and services" are, leading to legal uncertainty at least until the first cases will have been resolved in court.

In order to balance market power, **with Article 5(2) of the DA, the Commission tries to prevent further concentration of data at the gatekeepers denoted under the DMA, by making them ineligible to access data as a third party from other data holders even upon a user request or if being sub-contracted by the third party (DA, Recital 36).** Again with the aim of protecting data holders, this provision reduces data access to some of the most innovative companies and is a limitation to users' right to choose.

Concerning this issue, BEREC[20] stresses that it is important to address the possibility of gatekeepers bypassing this prohibition by buying data holding rights, instead of the data themselves. This arises from the difference between being the manufacturer of the "data collecting product" and being the data holder of the data generated by this product. Manufacturers can design products to forward collected data to storage other than at its producer's. As of this writing, no agreement on the exact delimitation of the prohibition has yet been reached in the trialogue negotiations. Relatedly, it not immediately clear where to draw the line between the acquisition by the gatekeeper of data rights, data, and the data holder's business itself, with implications for which will be the authority in charge.

SMEs receive special protections under the DA, to lower barriers for accessing data, again with the aim to stimulate competition. First, the DA exempts SMEs from the obligation to make data available to public authorities in cases of emergency, due to its cost. The DA also obliges data holders to limit the compensation asked from a data holder to an SME data recipient, stating that "any compensation agreed shall not exceed the costs directly related to making the data available to the data recipient". Lastly, SMEs will benefit from the contractual fairness clauses of the DA. In its impact assessment, the Commission estimates that the elimination of imbalances in bilateral contractual relations alone can boost SMEs' profits up to EUR 5.2 billion per year[21]. Still, CERRE[22] points out possible problems with this provision: For example, the size of the players involved is not necessarily connected to bargaining power; a position of economic or data dependence may provide smaller players with strong bargaining power.

The cost of compliance with the DA can be another issue. How will the burden to comply affect non-SME companies, and how will it change their behaviour? Will non-EU markets become relatively more attractive or non-EU firms relatively more competitive? Furthermore, the step change in applicable rules and implied investments may create a threshold effect for firms growing up from SME status.

[20] BEREC (2022), BEREC High-Level Opinion on the European Commission's proposal for a Data Act, BoR (22) 118, https://www.berec.europa.eu/en/document-categories/berec/opinions/berec-high-level-opinion-on-the-ecs-proposal-for-a-data-act.

[21] European Commission (2022), Study to support an impact assessment for the review of the database directive. https://copenhageneconomics.com/wp-content/uploads/2022/02/study-to-support-an-impact-assessment-for-the-review-of-the-database-directive.pdf

[22] CERRE (2023), Data Act: Towards a balanced EU data regulation. (www.cerre.eu)

1.4.3 Regulatory Dimension

Together with the DMA and DSA, **the EU Data Strategy forms part of a movement to set out tighter *ex-ante* rules for certain markets, instead of relying principally or solely on *ex-post* intervention by competition authorities.** While most of the framework is consistent with competition subject to *ex-post* enforcement, one clear aim is to avoid competition problems from the start and reduce the necessity for future intervention, in particular with respect to abuse of market power in bilateral relations. On the other hand, some of the measures, e.g. for voluntary sharing of data, may need closer cooperation between potential competitors, which goes against the grain of present competition policy. As is the case with network investment in electronic communications, finding the right balance may be difficult.

A data-driven Common Market can be expected to lead to further integration of value chains across sectors and Member-States. This may create both synergies in regulation between and the necessity to transform regulatory bodies within Member States, in different but overlapping areas such as privacy protection, competition, or telecoms. Member States may want to create cross-functional working groups drawing on these regulators, emulating the EDIB at national level, or even move towards merging some previously separate regulatory institutions, just as Spain did by merging the competition and telecoms agencies, or Germany by merging all network regulators into the Bundesnetzagentur.

While the EDIB will assist the Commission in implementing the Data Strategy, it remains to be seen whether it will also strengthen the cooperation between regulatory agencies of different Member States. It is also unclear whether any institution will address the social and ethical impacts of data use and related developments in AI under the existing framework.

Additionally, **the abundance of work that will result from the DA and DGA will require well-capacitated regulatory bodies**. The creation of effective competent national bodies will require a **significant investment in human resources and skills,** which is will certainly be costly and influence the power equilibrium in public administrations and regulators. The potential for the overlapping of attributions in the areas of privacy, data protection, cybersecurity, network infrastructure, and competition issues may create conflicts.

In establishing these competent bodies, **Member States may choose to create new regulatory entities or attribute new responsibilities to the existing ones.** In the DA, the Commission gives 12 months to the Member States to do this. BEREC[23] mentions the need of permanent dialogue between Member States in this process, and also the possible need to extend this deadline in some cases. It is important to question whether clearer guidelines are needed to harmonize the designation and capacitation of competent authorities.

On May 10th, 2023, the French government unveiled a legal proposal for the digital economy for the protection of users and businesses, including the transpositions of the DSA and DMA and parts of

[23] Ibid.

the European Data Strategy[24]. The proposal is a good example of the complex web of competent authorities that may arise at national level. Apart from the Competition Authority, the media regulator Arcom will enforce the DSA as “digital services coordinator” and be responsible for platform content under the DMA (apart from its role of suppressing pornography and hate speech). Also under the DMA, the Directorate-General for Competition, Consumer Affairs, and Fraud Control will oversee marketplaces, while the National Commission on Informatics and Liberty, the privacy regulator, deals with data protection issues. Under the DGA, the latter will also cover data donated in the public interest, the Interministerial Directorate for Digital Affairs will deal with public data, and Arcep, the communications regulator, oversees the data economy and data intermediaries[25]. Finally, at the implementation level, CERRE[26] points out that terms such as “pseudonymisation” and “anonymisation”, which are important for the rules about privacy protection, are used inconsistently in the DA. The DA also lacks rules to limit or prohibit problematic data usages such as re-identification and profiling techniques, among others. Even though privacy issues are also being addressed in other EU initiatives (concerning political speech, for example), it is important to remember that many rights enshrined in the DDR could benefit from more specific and stricter dispositions in the DA or any other of the above-mentioned acts, and from clarifications of their relationships in particular with the GDPR. Again, these issues presently are under active discussion in the trilogue negotiations.

[24] France (2023), Dossier de Presse: Sécuriser e réguler l’espace numérique. https://www.entreprises.gouv.fr/files/files/secteurs-d-activite/numerique/dp-pjl-securiser-et-reguler-lespace-numerique.pdf

[25] Euractiv (2023), France mulls new ‘frontline’ digital bill going beyond EU rules. May 10th. https://www.euractiv.com/section/platforms/news/france-mulls-new-frontline-digital-bill-going-beyond-eu-rules/

[26] CERRE (2023), Data Act: Towards a balanced EU data regulation. (www.cerre.eu)

Chapter 2: Geopolitical aspects of EU's Data Strategy

2.1 Why data is a major geopolitical factor

Data is one of the most valuable resources in today's global competition – but it is not yet seen as a global common that leads to collaboration. So far, global data flows are still governed through a maze of multilateral, bilateral, unilateral, and *ad hoc* rules, principles, and voluntary frameworks that are not always accepted or applied by all actors. Cross-border international collaboration on this issue is far limited, with ups and downs in the success of a common global agenda on data governance. Also, data governance is getting balkanized in blocs that propose different, if not contrasting, data models. Doing so is as important as strategic for the maintenance of an international security and peace order which growingly relies on the power over data and has strong impacts on three layers: security, economic, and rights.

The European Union's Data Strategy aims to make the EU a leader in a data-driven society[27]. The goal of creating a single market for data is to allow data to flow freely within the EU and across sectors for the benefit of businesses, researchers, and public administrations. However, the Data Strategy has much to do with the current debate over strategic autonomy -or digital sovereignty- and the way the EU needs to promote its global vision on technology through three lens: security, economy, and rights and values.

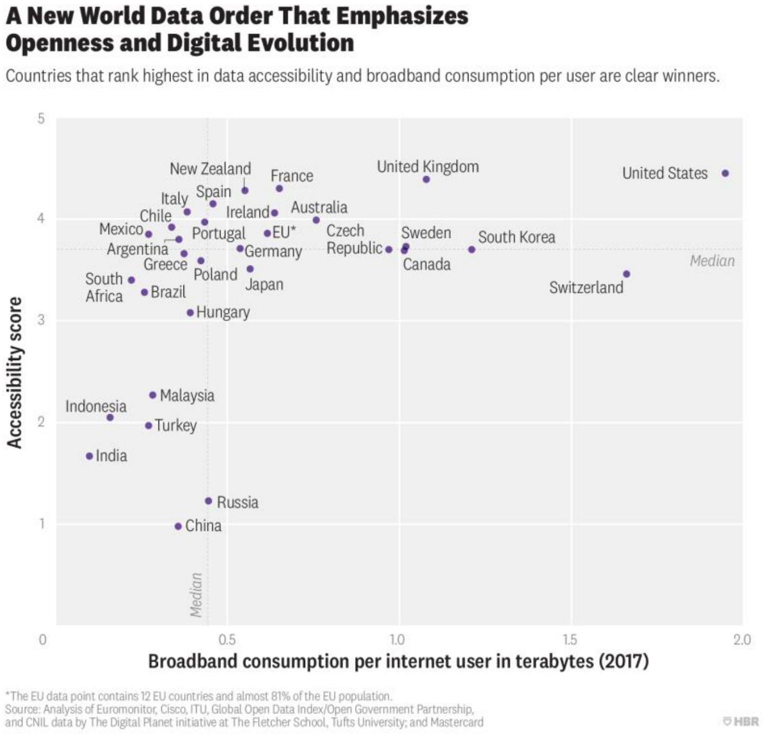
According to Harvard Business Review,[28] the countries that are leading the data economy worldwide are the United States, the United Kingdom, China, Switzerland, and South Korea. To estimate this, authors create a **new metrics that may measure the wealth and power of nations based on a new version of the "GDP": the Gross Data Product**. To identify the world's top "grow data product" producers, they consider four criteria[29]: the volume, usage, accessibility and complexity.

[27] European Commission (2023). The European Data Strategy. Accessible at https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_en

[28] *Chakravorti, B., Bhalla, A., Shankar Chaturvedi, R. (2019), "Which Countries Are Leading the Data Economy?", Harvard Business Review, 2019. Accessible at https://hbr.org/2019/01/which-countries-are-leading-the-data-economy*

[29] - Volume: Absolute amount of broadband consumed by a country, as a proxy for the raw data generated.
- Usage: Number of users active on the internet, as a proxy for the breadth of usage behaviors, needs and contexts.
- Accessibility: Institutional openness to data flows as a way to assess whether the data generated in a country permits wider usability and accessibility by multiple AI researchers, innovators, and applications.
- Complexity: Volume of broadband consumption per capita, as a proxy for the sophistication and complexity of digital activity.

Figure 1. Position per countries based on accessibility score and broadband consumption per Internet user



A New World Data Order That Emphasizes Openness and Digital Evolution

Countries that rank highest in data accessibility and broadband consumption per user are clear winners.

*The EU data point contains 12 EU countries and almost 81% of the EU population.
Source: Analysis of Euromonitor, Cisco, ITU, Global Open Data Index/Open Government Partnership, and CNIL data by The Digital Planet initiative at The Fletcher School, Tufts University; and Mastercard

Source: Chakravorti, B., Bhalla, A., Shankar Chaturvedi, R. (2019), "Which Countries Are Leading the Data Economy?", Harvard Business Review, 2019. Accessible at https://hbr.org/2019/01/which-countries-are-leading-the-data-economy

Still, **it remains complex to establish a ranking of "new" data leaders, as global leadership over data power cannot be only weighed in terms of who provides further accessibility. The current international system is witnessing an increasing authoritarian overhaul of data capture, storage, use and processing**. According to the *Freedom on the Net* 2022 report, which assesses 89% of the world's Internet user population, 37% of the population lives in countries with no Internet freedom, 34% live in partly free countries, and only 18% of user population lives in territories where Internet freedom is fully granted[30].

Global Internet freedom has declined for the 12th consecutive year, and **countries have applied several strategies to access, block, disrupt, and control data**. An increasing number of national governments have blocked websites, access to data, imposed new national laws on threats to the free flow of information, have centralized technical data infrastructure, have applied regulations with stricter data localization policies which centralize the governmental control over user data, or

[30] Freedom House (2022). *Freedom on the Net* report. Accessible at https://freedomhouse.org/sites/default/files/2022-10/FOTN2022Digital.pdf

impose companies to comply with national requirements -making them store data within the country, change their operations in a way that facilitate government censorship or requests to sensitive data, or prohibiting data users to bypass the "national digital walls" and access third countries' information. Also, restrictions and blocks on foreign websites have increased (in 2022, 37 countries did so) and 11 countries have approved new laws restricting these foreign websites and content.

These nationally driven data policies are having a major impact on how countries relate to each other, and how the global Internet is built. Censorship, filtering, market access restrictions, strict licensing regulations, joint-venture requirements, maximum foreign equity shares, nationality requirements and stricter obligations for foreign companies have led to **increasing barriers to the cross-border flow of data, a topic that has become geopolitically sensitive**, due to its impact on security, economic competitiveness, and fundamental rights.

The geopolitical competition has been placed at two levels: **the race over the harvesting of data, and the race over the usage of data.** Both have implications on how countries collaborate internationally, the political willingness to enter into international agreements on data flows (either personal or non-personal), and the much-needed role of "trust" to bundle a massive package of information and maintain international security and peace.

2.2 The EU's role in the geopolitics of data

It is by no chance that the EU has been addressing how their goods, services, assets, and personal data relate to third countries through several ways. The first approach is **regulation**, which has been closely followed by the majority of stakeholders. However, two other approaches are as important as strategic: **the role of multilateral initiatives, "coalitions of the willing" and international meetings; and the importance of technology diplomacy as a policy area to institutionalize the geopolitics of data, alongside other technological challenges.**

2.2.1 Through regulation

2.2.1.1 The General Data Protection Regulation (GDPR)

The EU's General Data Protection Regulation (GDPR) -the backbone of the EU Data Strategy- only permits the transfer of personal data to those jurisdictions that comply with a sufficient level of data protection. Article 45 gives **the European Commission the power to determine whether a country outside the EU offers an adequate level of data protection**[31]. The effect of such a decision is that personal data can flow from the EU -and three Associated Countries: Iceland, Liechtenstein, and Norway- to the third country without any further safeguard being necessary.

[31] https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

So far, the so-called "data adequacy decisions" have been recognized in Andorra, Argentina, Canada (for commercial organizations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Republic of Korea, Switzerland, the United Kingdom, and Uruguay. All data adequacy decisions exclude data exchanges in the law enforcement sector, except for the United Kingdom.

Data adequacy provisions have as admirers as critics. On the one hand, it is perceived as a guardrail that ensures the protection of fundamental rights, the influence over third countries to develop norms which respect democratic values, and as a geopolitical tool to gain leadership over the global agenda on cross-border data flows. The GDPR is widely considered a blueprint for data privacy, often referred to as the "gold standard"[32] for international data usage, as an increasing number of countries tend to mimic the principles and structure of this regulation[33]. This would follow the Brussels Effect[34] approach, which explains how EU regulatory power is externalized, influences the behaviors of foreign governments and companies, and induces the framing of certain global norms. On the other hand, data adequacy provisions have also received criticism because their standards may lead certain governments to "mandate domestic data storage, feature blanket exceptions for national security or state actors without safeguards, or delegate increased decision-making power to politicized regulators—all of which renders users vulnerable to government abuse despite improvements pertaining to the use of personal data for commercial purposes"[35].

2.2.1.2 Data Services Act (DSA) and Digital Markets Act (DMA)

The final texts of both the DSA and the DMA were a thermometer of how the EU aimed to tackle its relationship with actors from third countries. While the major impact of these rules is on the internal single market, the reality is that it addresses many aspects of digital sovereignty -capabilities of states, respect to human rights, and economic leadership.

With regards to the DSA, the imposition of measures over Very Large Online Platforms[36] features how the EU is touching the behavior of these companies, which mostly come from China and U.S. jurisdictions[37]. The goal is three-fold: protect rights (citizens' rights from increased risks and harms), guarantee security (through content moderation to avoid harmful messages, or to cause damages), and foster a competitive economy (removing barriers for trade in digital services and protecting

[32] Buttarelli, G. (2016). The EU GDPR as a clarion call for a new global digital gold standard. *International Data Privacy Law 6*(2), 77-78. https://doi.org/10.1093/idpl/ipw006.

[33] Luisi, M. (2022). GDPR as a Global Standards? Brussels' Instrument of Policy Diffusion. Accessible at https://www.e-ir.info/2022/04/09/gdpr-as-a-global-standards-brussels-instrument-of-policy-diffusion/

[34] Bradford, A. (2020). *The Brussels effect: How the European Union rules the world*. Oxford University Press, USA.

[35] Freedom House (2022). *Freedom on the Net* report. Accessible at https://freedomhouse.org/sites/default/files/2022-10/FOTN2022Digital.pdf

[36] European Commission (2023). *Digital Services Act: Commission designates first set of Very Large Online Platforms and Search Engines*. Accessible at https://ec.europa.eu/commission/presscorner/detail/en/IP_23_2413

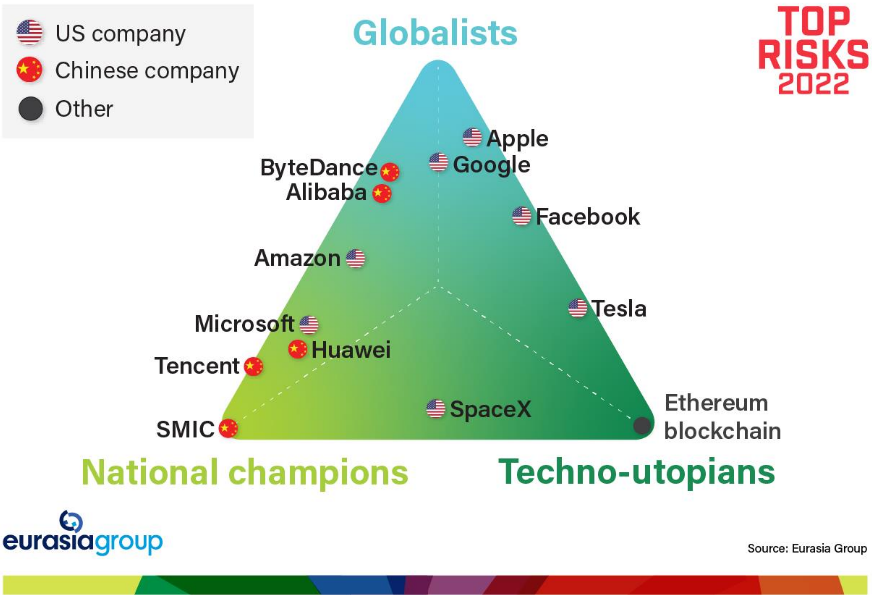
[37] Freihse, C., Overdiek, M. (2022). Digital Services Act and Digital Markets Act: Towards European Digital Sovereignty? *GED*. Accessible at https://globaleurope.eu/europes-future/digital-services-act-and-digital-markets-act-towards-european-digital-sovereignty/

SMEs, which are the bulk of companies at the EU). As for the DMA, the main aspect on digital sovereignty was how to reduce market concentration and ensure fairness in business practices.

However, **the main challenge for the EU to deploy this regulatory tool as a geopolitical asset relies on whether the EU will get to influence other countries to follow the same approac**h. It is not only about imposing certain rules to those that already do interact with the EU, but about encouraging others to do the same with their owns. This might explain why the EU launched in 2022 a new Tech Office in San Francisco with a Senior EU Envoy for Digital to the U.S., whose portfolio aims to create public acceptance of this regulation as a positive tool for international collaboration.

Similarly, another challenge for the geopolitical instrumentalization of these regulations is to understand that **geopolitical strategies should vary depending on the country and type of technology company, as firms may have different geopolitical approaches**.

Figure 2. Three types of global technology companies, by attitude



Source: Eurasia Group (2022)[38]. Top Risks 2022

The way of addressing the geopolitics of technology in general, and of data in particular, is not only about the governmental rivalry between China and the United States. It is also about each technology company, as companies coming from the U.S. see the world through different lens. This is why the Eurasia Group divides firms in three main types:

- **Globalists**. Firms that built their power by operating on an international scale, settling down across countries and competing intensively. This is the case of Apple, Facebook, and Google, whose services go beyond national borders and outside from physical territory. They aimed

[38] *Eurasia Group (2022). Top Risks 2022*. Accessible at https://www.eurasiagroup.net/live-post/top-risks-2022-2-technopolar-world

to dominate a specific market niche and to extend it globally. Alibaba, ByteDance, and Tencent followed the same pattern, first dominating the Chinese market, second expanding it worldwide.

- **National champions**. Some globalists were -and are- national champions that first grew at the national level. What differs is that the category of "national champions" refer to those companies that are more willing to align themselves explicitly with the priorities of their home governments. These firms are partnering with governments in various important critical technology domains. Main cases come from China, such as Huawei and SMIC. In the U.S., globalist companies emerged after being national champions, such as Amazon and Microsoft, which compete to provide cloud-computing infrastructure to the U.S. government.
- **Techno-utopians**. These firms see technology not just as a global business opportunity but also as a potentially revolutionary force in human affairs, beyond the nation-state paradigm. This type tends to center on the personalities and ambitions of technology CEOs rather than the operations of the companies themselves. This might be the case of Tesla and SpaceX.

Still, there are **divided opinions on whether technology firms are or not geopolitical actors**. Some experts argue that they play a major role[39] in geopolitics because they are creating new topics to be dealt at the highest levels of decision-making, and they are receiving attention from governments (either positively or by imposing regulations on them). Others argue that they cannot be categorized[40] as geopolitical actors because the international order is still largely marked by physical challenges, such as refugee flows, drought and war.

In any case, EU's regulation over markets and competition has had an important effect on the way technology firms act in EU territory.

2.2.1.3 Data Act

The Data Act is perceived as the opportunity for the manufacturing industry. Platforms generate data, but Data Act is aimed at the usage of this data by the manufacturing sector. It is a horizontal legislation, so it affects all sectors.

While it may be seen only as a single market-oriented regulation, the reality is that it aims to influence the way the EU harness its strategic autonomy or digital sovereignty with third countries and actors.

Two critical points exist on this matter. First, **with regards to Intellectual Property**, as the European Commission's definition in their first proposal left an open definition, the European Parliament had to refine the definition. **Since the definition of "trade secret" cannot be changed because it is closed, the Parliament decided to focus on the definition of "data"** (this is, the scope of what is

[39] Bremmer, I. (2021). The technopolar moment: How digital powers will reshape the global order. *Foreign Aff.*, *100*, 112.

[40] Walt, S. (2021). Big tech won't remake the global order. *Foreign Policy*, *8*.

included and what is not). While raw data will always fall under the obligations of the regulation, it has to be readable to avoid a lack of usability and misinterpretation of the data received. On the other hand, data which are the function of (sophisticated) processing will be excluded in order not to hamper previous investment and respect IP rights and trade secrets.

Second, **defense-related data has been excluded because it raised concerns over the potential weaponization of the Data Act by certain companies from third countries**. Airbus has been excluded from the Data Act as it handles with sensitive information from the defense sector.

In both cases, a geopolitical risk that the Data Act aims to prevent from is that companies from third countries complying with the regulation might use economic security policies to enter into the European market with less guardrails. In this line, **it will remain important to make sure that the Data Act is effectively aligned with the export control regimes currently agreed at the EU level.** However, more than this, it will be paramount to guarantee that the interpretation and implementation of those export control standards by Member States -which are the final policy shapers of this regime- are carried out in a harmonized, transparent, and comprehensive manner to prevent risks. These export control regimes should tackle high-technology services and sensitive data that is shared.

Similarly, the **EU should carry out a risk assessment on the weaponization of data to affect EU's priorities, interests and vision based on the three primary streams of data that are available for harvesting**: user-generated content, information purchased from Original Data Suppliers (ODS), and third-party data services from intermediaries[41].

2.2.1.4 Data Governance Act (DGA) and European Data Spaces

The DGA aims to increase trust in data sharing, strengthen mechanisms to increase data availability and overcome technical obstacles to the reuse of data. The main output of the DGA is the development of common European data spaces in strategic domains, such as public administration, health, environment, energy, agriculture, mobility, finance, manufacturing and skills.

The main vision of the European data spaces is to create the idea of "sovereign data ecosystems", governed by a cross-sector common infrastructure of cloud, data, and AI. It relies on federated communities, the value of trust (transparency and compliance across all spaces), innovation, and the generation of economic competitiveness. The final goal of creating a federated community and fostering trust is to contribute to the EU's role of strategic autonomy.

2.2.1.5 International data transfers: the case of the EU-US transatlantic framework

After the blockade of the Privacy Shield in July 2020 by the Court of Justice of the European Union due to EU's concerns over the misapplication of the transatlantic data flows framework by the

[41] Capri, A. (2022). Geopolitics and the race for data supremacy. *Hinrich Foundation*. Accessible at https://www.hinrichfoundation.com/research/wp/tech/geopolitics-and-data-supremacy/

United States, in 2022 the two sides announced that they had reached an agreement on a new EU-U.S. Data Privacy Framework. With President Biden's Executive Order from October 2022 on 'Enhancing Safeguards for United States Signals Intelligence Activities', the introduction of new binding safeguards to address all the points raised by the EU Court of Justice, limiting access to EU data by U.S. intelligence services and establishing a Data Protection Review Court, the European Commission is preparing a draft adequacy decision to be adopted soon[42].

However, regulation is not the single approach that the EU should take in the geopolitics of data. To do so, two other approaches are as important as strategic: the role of multilateral initiatives, "coalitions of the willing" and international meetings; and the importance of technology diplomacy as a policy area to institutionalize the geopolitics of data, alongside other technological challenges.

2.3 The role of multilateral initiatives and "coalitions of the willing"

The exposure to threats and opportunities in the weaponization of data cannot be only addressed through the lens of regulation. This is why countries are increasingly moving up their proposals on data to the level of multilateral meetings.

These meetings may be divided in two types: **institutionalized organizations and spaces with long-lasting history, and *ad hoc*, recent coalitions** which are aimed at pushing forward specific, tailored topics, at specific speeds, and through expected deliverables.

On the first group, the most prominent ones are the G7 - the informal grouping of seven of the world's advanced economies, including Canada, France, Germany, Italy, Japan, the United Kingdom, and the United States, as well as the European Union, which participates but has no vote capacity -, the United Nations -which is hosting the Special Envoy on Technology and the implementation of the Roadmap on Digital Cooperation as well as the UN Global Digital Compact -, the OECD -which devotes initiatives to data policy, such as the Declaration on Trusted Government Access to Data[43], and also to Artificial Intelligence, such as OECD.AI and the Global Partnership on AI -, and regional organizations such as the African Union, ASEAN -with its Digital Masterplan- and regional development banks that are arranging discussions over data policies and the importance of multilateral collaboration.

On the second group, countries are inching toward creating alliances with like-minded countries on a bilateral or multilateral basis. Most prominent examples are the Quadrilateral Security Dialogue or Quad -U.S., Australia, India and Japan-, which leverage the collaboration on data to activities[44] such as maritime security (for example, by providing near-real-time, integrated maritime domain data to maritime agencies in Southeast Asia and the Pacific), Earth Observation data (to ensure

[42] European Commission (2022). *Questions & Answers: EU-U.S. Data Privacy Framework*. Accessed on May 24, 2023. Accessible at https://ec.europa.eu/commission/presscorner/detail/en/qanda_22_6045

[43] OECD (2022). Declaration on Government Access to Personal Data Held by Private Sector Entities. Accessible at https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0487

[44] White House (2023). *Quad Leaders' Joint Statement.* May 20, 2023. Accessible at https://www.whitehouse.gov/briefing-room/statements-releases/2023/05/20/quad-leaders-joint-statement/

peaceful, safe and sustainable use of outer space), or data analysis to map threats to supply chain disruptions or resilience in critical technologies.

It is also the case of the Digital Economy Partnership Agreement or DEPA -composed of Chile, New Zealand, and Singapore to tackle digital trade challenges. China aimed to join DEPA in the past in this strategic partnership based on partnerships between Latin America, Southeast Asia and Oceanic.

Other initiatives have been launched – D-10[45], Tech-10[46], T-12[47] -, but with limited success, complete failure, or ineffectiveness[48] due to expectations mismatch, lack of delivery, or too simple low-hanging fruits that did not provides the needed incentives for actors to keep collaborating.

In all cases, data has been addressed through several lens: data privacy, cross-border flows of industrial, non-personal data (which impinges on the core of critical infrastructure, critical technologies, and economic security instruments such as export controls and Foreign Direct Investment), how to foster R&D and joint consortiums across countries with sensitive or critical data, or the impact of data usage on fundamental rights.

In the case of the EU, the Union has participated in several initiatives, particularly the G7 and G20. Some initiatives have been particularly critical for the geopolitics of data. In 2019, the then-Prime Minister Abe Shinzo from Japan proposed, during its Presidency of the G20, the Data Free Flows with Trust (DFFT) approach to guarantee the enhancement of cross-border data flows, based on the combination of privacy and security of personal and sensitive data. As the data governance approach is getting balkanized by blocs which propose different, if not contrasting, data models - see China's state-controlled model, the EU's regulation focus, and the U.S. liberal approach-, Japan decided to pursue a new proposal based on an interoperable global governance of the data, that ensures the promotion of free data to foster economic growth as well as the protection of individual privacy, national security, and Intellectual Property rights through trusted regulations.

Since the Declaration supporting the DFFT model in 2019, Japan has advanced the concept in several ways[49], also with the support from the European Union. For example, in April 2021, the G7 launched a Roadmap for Cooperation on DFFT[50] which focuses on four streams: data localization, regulatory cooperation, government access to data, and data sharing for priority sectors. This roadmap was

[45] Brattberg, E., Judah, B. (2020). Forget the G-7, Build the D-10. *Foreign Policy.* Accessible at https://foreignpolicy.com/2020/06/10/g7-d10-democracy-trump-europe/

[46] Manuel, A. (2020). The Tech 10: A Flexible Approach for International Technology Governance. Accessible at http://anjamanuel.com/new-page-40

[47] Cohen, J., Fontaine, R. (2020). Uniting the Techno-Democracies: How to Build Digital Cooperation. *Foreign Affairs* (November/December 2020). Accessible at https://www.foreignaffairs.com/articles/united-states/2020-10-13/uniting-techno-democracies

[48] Rasser, M., Arceasti, R. Oya, S., Riikonen, A., Bochert, M. (2020). Common Code: An Alliance Framework for Democratic Technology Policy. *Center for A New American Security.* Accessible at https://www.cnas.org/publications/reports/common-code

[49] Arasasingham, A., Goodman, M. (2023). Operationalizing Data Free Flow with Trust (DFFT). *CSIS*. Accessible at https://www.csis.org/analysis/operationalizing-data-free-flow-trust-dfft

[50] G7 Roadmap for Cooperation on Data Free Flow with Trust (2021). Accessible at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/986160/Annex_2__Roadmap_for_cooperation_on_Data_Free_Flow_with_Trust.pdf

translated into an Action Plan[51] to promote the DFFT. The implementation has been also materialized in bilateral agreements, such as the Japan-U.S. Digital Trade Agreement, the Japan-UK Comprehensive Economic Partnership Agreement, and the EU-Japan Digital Partnership Agreement. **While cooperation with U.S., UK, EU, Canada and like-minded countries is straightforward, the main challenge lies in how to agree on policies to counter the proliferation of data localization policies with those countries where Japan would aim to partner with, but have different opinions on this issue. A paradigmatic case is India**, which is part of the G20 and, during the preparation of the declaration supporting the DFFT in 2019, was against this statement. India argued that the DFFT approach was not comprehensive enough in the legislation of its country, and could lead to inequalities across developing and developed countries. However, it is important to note that India is one of the countries that has invested much more efforts in data localization policies worldwide, what explains its opposition to the DFFT model.

This is why the EU has an opportunity[52] to partner with Japan and engage closely with the Indo-Pacific region. Japan is gaining traction in *ad hoc* coalitions –from the Quad to Blue Dot Network– and has also been proactive in pursuing technology principles as well as leading relevant ecosystems –such as GPAI, Osaka Track and the PQII–. At the same time, the country also relies on traditional multilateral settings as it aims to seize leadership in Asia by means of regional cooperation and on some previous attempts to reach out to African governments jointly with India. However, Japan's approach to technology competition is cautious: it does not intend to become confrontational with China. This places it in an inter-theatre position where it has opportunities to cooperate with the EU to project a democracy-affirming technology governance at the multilateral level without renouncing to cooperation with China when deemed appropriate.

2.4 The building-up of EU's technology diplomacy

The European Union has been developing its foreign policy on technology since several years. It has done it in three main forms. First, by strengthening the number and scope of technical assistance projects in third countries -mostly through the Directorate General of International Partnerships, which was before the development cooperation branch of the European Commission. Second, by launching a number of regional initiatives with specific partners, focused on digitalization. Third, by setting up the first-ever framework on Digital Diplomacy in July 2022. The two latter are analyzed.

2.4.1 Regional initiatives for technology partnerships

[51] G7 Action Plan for Promoting Data Free Flow with Trust (2022). Accessible at https://bmdv.bund.de/SharedDocs/DE/Anlage/K/g7-praesidentschaft-final-declaration-annex-1.pdf?__blob=publicationFile

[52] Jorge Ricart, R. (2022). The EU and Japan: forging joint opportunities for global technology governance beyond great power rivalry. *Elcano Royal Institute*. Accessible at https://www.realinstitutoelcano.org/en/analyses/the-eu-and-japan-forging-joint-opportunities-for-global-technology-governance-beyond-great-power-rivalry/

Alongside the Digital Partnership Agreement with Japan, the EU has established a number of regional initiatives with third countries and regions where data is a key focus of the discussion:

- **EU-U.S. Trade and Technology Council**, which serves as a "forum for the European Union and the United States to coordinate approaches to key global trade, economic, and technology issues and to deepen transatlantic trade and economic relations based on shared democratic values".

The TTC has ten Working Groups, out of which one is devoted to data governance and platforms, and others address technology standards cooperation, where data is approached to create joint roadmaps on evaluation and measurements tools to create trustworthy Artificial Intelligence. Also, data is approached by the Working Group on ICT security and competitiveness, which decides on how to address security risks from high-risk vendors and suppliers. Likewise, the Working Group on "Misuse of Technology Threatening Security and Human Rights" has four main areas of work: (1) combatting arbitrary or unlawful surveillance; (2) protecting human rights defenders online; (3) technical and diplomatic coordination to Internet shutdowns; (4) identification of state-sponsored information manipulation and interference. Their cooperation goals refer to info-sharing, joint mapping of risks and support with techniques to identify vulnerabilities, by leveraging data.
Additionally, in December 2022 the TTC agreed on joint infrastructure and connectivity projects globally, concretely in Jamaica (connecting to the Internet 1000 public schools and children's homes) and in Kenya (expanding Internet access for schools), which will leverage the EU and U.S. approach to data flows and governance in third countries.

- **EU-India Trade and Technology Council**, which aims to establish India as a strategic partner after several years of blockade of their diplomatic relationships. This is framed in the revamped negotiation over a bilateral Free Trade Agreement. Out of the three working groups, one is devoted to strategic technologies, digital governance and digital connectivity, where both sides aim to discuss about the role of data for Digital Public Infrastructures and some industrial data spaces -but no discussions on data localizations have been set up so far, due to differences on this vision.

- **Digital Partnership Agreements (DPAs) with Japan, Republic of Korea, and Singapore.** As the Japan's DPA has been explained, the main goal of the DPA with Korea is to guide the governance of data through the values of freedom and human rights, as well as to ensure solidarity for the freedom of digital citizens in their use of data to protect rights. The DPA with Singapore does not focus on rights, but rather on the leverage of data for digital trade, 5G and 6G, online platforms, SMEs digital transformation, fintech, digital skills and standards.

- **Digital Agenda for Western Balkans.** Out of the four areas of work, three are devoted to data: investing in broadband connectivity and its roll-out; strengthening the digital economy and society through the deployment of open data and digitalization of the public administration and procurement processes; and boosting research and innovation by promoting data usage for R&D.

- **Eastern Partnership's EU4Digital Initiative.** Main areas of data governance are the development of regulatory convergence in telecom rules, trust and security, eHealth and eSkills. Central to the EU4Digital Initiative is the three-year EU-funded EU4Digital Facility (2019-2022), or EU4Digital Facility, which promotes key areas of the digital economy and society, in line with EU norms and practices, and communicates EU support across the digital agenda in the region.

- **Joint Commitment to Digital Transformation in the EU-Africa Joint Vision for 2030.** This partnership aims to provide a win-win approach and agreed tangible outcomes, which includes an Africa-Europe Investment Package of at least EUR 150 billion that will support their common ambition for 2030 and AU Agenda 2063, enhancing digital infrastructure and facilitating digital transformation. Also, the **EU-Nigeria Digital Economy** Package, under the Global Gateway initiative, is planned to invest at least €820 million in Nigeria's digital transformation. With a combination of €160 million in grants and €660 million in loans, the EU aims to comprehensively support Nigeria's digitalization strategy.

- **EU-Latin America and Caribbean Digital Alliance.** Launched in March 2023, it aims to be a platform for an institutionalized dialogue at both the political and working levels on digital challenges and opportunities for both regions. The four areas of work align with the leverage of data as a geopolitical tool of cooperation: regulatory and policy cooperation, extension of connectivity infrastructures, innovation and private sector cooperation, and digitally-enabled products and e-services.However, still it remains to be seen how this alliance will be translated into specific outcomes, as LAC countries have strong differences on the political willingness and approach to deal with the UE in digital issues. Likewise, no political declaration was made during the launch day of the alliance. Additionally, the Digital for Development (D4D) Hub that accompanies this Alliance will need to deliver further publicly available outcomes, such as monitoring of needs and the actual implementation of actions.

- **Global Gateway.** This infrastructure investment initiative led by the EU, which aims to accompany the Build Back Better World (B3W) by the U.S. and be an alternative to the Chinese Belt and Road Initiative, ranks digitalization as its first priority out of five. There are six references to specific data-oriented initiatives. These are the deployment of digital networks and cloud and data infrastructures with partner countries, the promotion of green data centers, the deployment of underwater cables equipped with ocean monitoring sensors, the offering of digital economy packages that combine infrastructure investments with country-level assistance on ensuring the protection of personal data, and international cooperation on data protection under the EU-LAC Digital Alliance.

2.4.2 The first-ever framework on Digital Diplomacy

Technology and digital policy have been long addressed as an economic issue. In 2019, the EU started to look at technology through the lens of "ethics" -see the High-Level Expert Group on AI Ethics-, and as a political and geopolitical issue. This explains why the DG INTPA's Unit on Science, Technology, Innovation and Digitalization was pushed forward in early 2020, although it mainly focuses on technical assistance projects. No strong political decisions have been made at the highest level of decision-making, and human rights have been limitedly included in the political and policy discussion.

The EU Council Conclusions on digital diplomacy from July 2022[53] is the **landmark, the starting point, for the EU to 'institutionalize' all things related to the external agenda in third countries on digital policy as a single line of foreign policy by the EU**. The wording 'digital diplomacy' aims to put all scattered initiatives that had been done so far into the same box.

Digital policy is no longer only a domestic issue. It is also part of the foreign policy agenda. It is not about digitalizing the diplomatic communications or protecting the information that flows through diplomatic corps. It is about identifying how a country aims to protect, promote and guarantee their vision about the world, about the international order, and how to govern technology to do so.

In the specific case of data geopolitics, the EU Council Conclusions address the geopolitics of data in several aspects.

- First, how to address the role of "trust" in data governance with third countries.
- Second, how to support European businesses' global reach and promote European examples of ethical approaches to data usage, since responsible use of data by businesses and governments forms the basis for the development of trustworthy and responsible digital ecosystems.
- Third, how to improve the EU's capability to monitor global digital regulatory activity, international data flows and the data privacy of EU citizens, patterns of digital trade, partnerships between third countries and their effects on the competition framework in the global market for digital technologies and services.
- Fourth, the leverage of datasets for EU outer space goals and security and defense.

[53] European Union Council (2022). *Council Conclusions on EU Digital Diplomacy*. Accessible at https://data.consilium.europa.eu/doc/document/ST-11406-2022-INIT/en/pdf

- Fifth, how to commit relevant instruments and funding to combat Internet shutdowns, arbitrary or indiscriminate digital surveillance and data retention alongside a concerted policy to promote human rights online e.g. through Human Rights dialogues, to protect human rights defenders and civil society online and expand civic space.
- Sixth, how promote digitalization and data sharing in favor of sustainability and the SDGs in governments and the private sector.

Still, to govern the geopolitics of data, it would be recommended that the EU adds up new activities much more oriented to restrictive measures and punishment initiatives. For example, how to condemn, sanction or apply conditionality requisites when the EU partners with a third country that violates certain principles, rules or rights that are on the top priority of the Union. Likewise, there should be further lines of action on mapping of risks derived from the cooperation with certain third countries. Also, digital diplomacy might tackle whether or not EU call for tenders' criteria should be stricter when it comes down to public procurement and risk assessment, mostly from those companies that store, collect and capture data that might be sensitive if transferred to a third country.

Alongside this challenge on the scope of ambition -which may increase over time-, there are three additional challenges.

First, **how to address the role of EU member states in the geopolitics of data**. Most foreign and security policy mandates depend on the unanimous support by all 27 countries at the EU Council. This might difficult how certain data governance activities might be approved. Also, member states tend to address international governance over data through the lens of purely regulatory issues -or economic issues-, but limitedly in terms of security and foreign policy. Likewise, member states largely differ in four areas when it comes down to how to interact in the geopolitics of data:

(1) political willingness (to include data as a new line of their foreign policy);

(2) situational awareness (about the importance of data in human rights and security);

(3) they have limitedly evaluated and addressed the risks of data on rights. This topic has not been included in National Action Plans on Business and Human Rights. Also, the EU Declaration on Digital Rights and Principles[54] is positive that was launched in 2022 is a positive effort, although it still requires to be mandatory and more influential across countries;

(4) Currently it would be difficult to find complementarity and coherence across EU member states' external tech policy initiatives. Most of the work led by the (few) existing tech ambassadors in EU territory do focus on business, R&D and entrepreneurship. The lens of security and rights is far limited if compared to economy.

[54] European Commission (2022). European Declaration on Digital Rights and Principles. Accessible at https://digital-strategy.ec.europa.eu/en/library/european-declaration-digital-rights-and-principles#:~:text=The%20Declaration%20on%20Digital%20Rights%20and%20Principles%20presents%20the%20EU's,version%20of%20the%20Declaration%20available

Second, a **key challenge for the EU is how to partner with developing countries or, particularly, digitally non-aligned countries**[55]. While there is still no movement similar to the formation of the Non-Aligned Movement in 1961, which was the product of not wanting to enter into geopolitical affiliations at a time of great powers rivalry, there are some dynamics that are pointing out to certain countries that might have the incentives to relook at traditional notions of non-alignment. This issue is still largely uncovered, but should be an area to delve into.

Three, all digital diplomacy branches should pay attention to certain technologies that are still underdeveloped, not too marketized or not in place, but that could generate major competition across countries. For example, a Chinese state-owned think tank flagged national security risks of metaverse[56], considering potential political and social issues. Metaverse will be fed by data, both personal and non-personal, from a large array of sectors ranging from healthcare and education to political advertising and retail.

2.5 Conclusion

Data is one of the most valuable resources in today's global competition – but it is not yet seen as a global common that leads to collaboration. So far, global data flows are still governed through a maze of multilateral, bilateral, unilateral, and *ad hoc* rules, principles, and voluntary frameworks that are not always accepted or applied by all actors. Cross-border international collaboration on this issue is far limited, with ups and downs in the success of a common global agenda on data governance.

The European Union is developing an increasing package to address the governance of data globally speaking. To do so effectively, it will need to face a number of challenges -from the perspectives of security, economy, and rights- that are not always framed under the existing policies. New scope, intensities, stakeholders' engagement and a higher level of ambition and monitoring will be the drivers to make the EU's leverage of its Data Strategy worldwide successfully with partners.

[55] Reddy, L., Soni, A. (2021). Is There Space for a Digital Non-Aligned Movement? *Cyberstability Paper: Series New Conditions and Constellations in Cyber*. Accessible at https://hcss.nl/wp-content/uploads/2021/09/Is-There-Space-for-a-Digital-Non-Aligned-Movement.pdf

[56] China Institute of Contemporary International Relations (2021). *The Metaverse and National Security*. CICIR.

Chapter 3: The economic impact of data-driven Innovation in Europe

3.1 A short introduction to Data-Driven Innovation and Data Economy

Data-Driven Innovation refers to innovation generated by the collection, processing and elaboration of data. According to the OECD definition (2015), "data-driven innovation involves the use of data and analytics to improve or foster new products, processes, organisational methods and markets"[57].

Businesses and other types of organizations have always relied on data to keep record of their activities and make them more efficient. However, data coding and storage, as well as processing, was limited. Only over the most recent decades, has technological progress, mostly related to Moore's Law, allowed for a huge amount of data to be available for collection, storage and manipulation at rapidly decreasing costs. More computational data is now generated any single day than up to the year 2000.

The data economy, based on data-driven innovation, has become increasingly pivotal to competitiveness and strategic autonomy.

To create value from data it is necessary to aggregate data or data insights from different applications, locations or external data spaces. How well this is done depends on the sophistication of algorithms and other important factors such as infrastructure (ultrabroadband & 5G, data centers, etc.), human skills, the right culture and internal governance and, of course, data availability. However, as economist Hal R. Varian famously stated, "many companies have data: they just don't know what to do with it. Missing ingredients: data tools (easy), knowledge (hard), experience (very hard)"[58].

Knowledge and experience grow with **experimentation**. In a physical world, experiments are very costly. Polls and focus groups are a proxy frequently used by companies and other organizations, but they are heavily affected by biases being based on opinions. Experiments are very easy to run in the digital world and have the important advantage of being based on real behavior of a large but easily identifiable group of users[59].

Big Data (i.e. large datasets to train large language models) **is an important asset, but also possessing the "right" data** (smaller datasets but highly relevant to the business/collecting purpose) should not be underestimated.

[57] OECD (2015), *Data-Driven Innovation. Big Data for Growth and Well-Being*, OECD Publishing, Paris.

[58] H.R.Varian (2013), *Beyond Big Data*, presented at the NABE Annual Meeting, September 10, 2013, San Francisco.

[59] S.Klepper (2016), *Experimental Capitalism: the nanoeconomics of American high-tech industries*, Princeton University Press, Princeton; S.H.Thomke (2020*), Experimentation Works. The surprising power of business experiments*, Harvard Business Review Press, Cambridge, Massachusetts; S. Stephens-Davidowitz (2017), *Everybody Lies. Big Data, New Data, and What the Internet Reveals About Who We Really Are*, Dey Street Books, New York.

3.2 Data Economy Overview: comparison between the EU and non-EU countries (US and China)

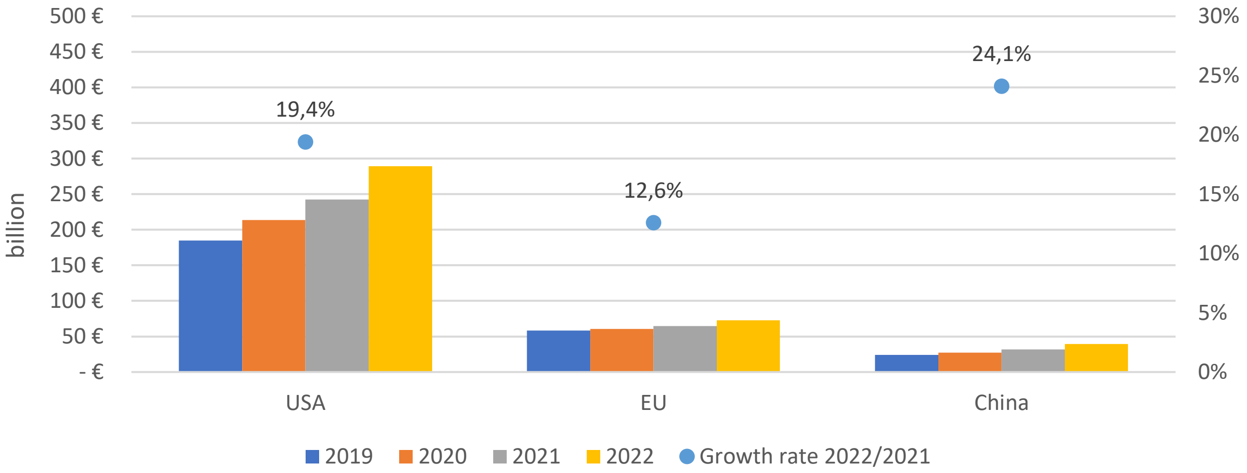
The development of technologies, such as the Internet of Things, smart devices and software applications, has led to an exponential growth in the volume of data generated by both organizations and individuals. Data analytics has opened up a world of opportunities for organizations that can leverage information to tailor their business to market demand. More and more organizations are recognizing the value possessed by data and are working towards its efficient and effective management, increasingly consolidating themselves in data-driven business models. Given the importance that data is assuming, its management is one of the keys to technological supremacy. For this reason, it is important to analyze how the EU is positioning itself in this field compared to other large economies such as the USA and China.

According to what emerges from the latest version of the report "European DATA Market Study 2021–2023" prepared by IDC on the initiative of the European Commission published in February 2023, in 2022, the **US continued to be the dominant player in the global data economy**. While the **hardware** sector was also strong, much of it being **manufactured outside the country**, with the primary source of the US's strength in the data economy being its advanced tools and software. As the world's largest economy, the US possesses the necessary resources and expertise to maintain its dominant position in data development and the data marketplace. **The US data market value in 2022 stood at €289.5 billion, nearly four times that of the EU (€73 bn) and more than seven times that of China (€40 bn)**. The data market is defined as “the marketplace where digital data is exchanged as products or services as a result of the elaboration of raw data. The data market captures the aggregate value of the demand of digital data without measuring the direct, indirect, or induced impacts of data in the economy as a whole”[60]. The US trend was confirmed in 2022 with year-on-year growth rates of 19.4%, while the EU occupied second position in terms of size and strength of the data market and data economy if compared against the present international background (Fig.3).

Despite its second position in absolute size, Europe (+12.6%) ranks lower than China in terms of percentage change. China has significant growth opportunities in this market, reporting a positive change of 24.1%. Despite the size of China's economy, its data market is relatively small. However, the rapid rate at which it is growing indicates that China has the potential to become a dominant player in the global data market in the coming years. This is due to the country's growth trends and the large number of data user companies it can accommodate. China's emphasis on developing data skills and investing in AI technology is poised to turn its data market into an important opportunity for companies offering data tools, data, and data services. Meanwhile, the US demonstrated steady growth in its data market during 2021-2022, confirming a consistent trend that is expected to continue despite the macro-economic challenges of the past two years.

[60] European data market study 2021-2023, Second report on facts and figures, February 2023

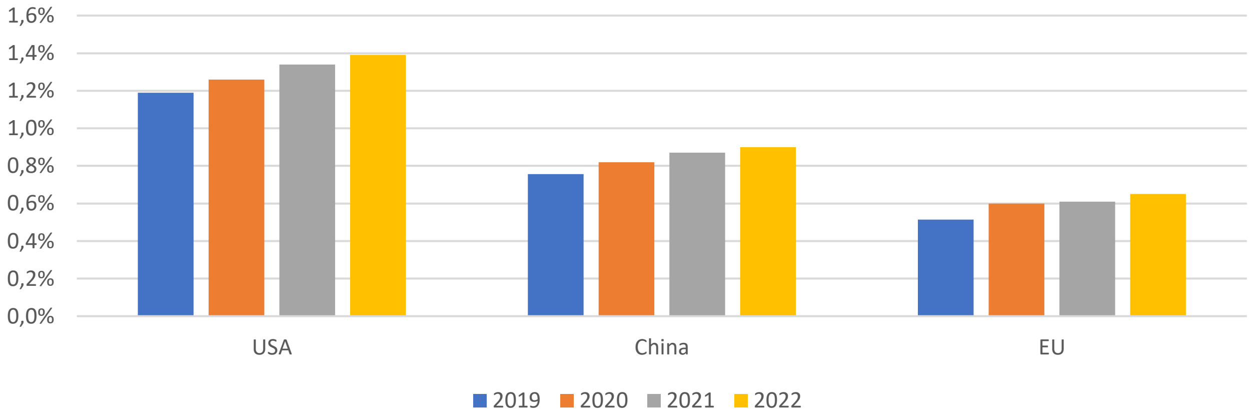
Figure 3: Value of the Data Market, by geographical area



Source: IDC, European DATA Market Study 2021–2023 (Second Report, February 2023)

Referring to the incidence of the data economy on the total economy, it is immediately clear that **the EU data economy's share on GDP is among the lowest of the Internationals** (Fig. 4). In this case, only the direct impacts[61] are taken into consideration. The greatest impact on GDP is recorded in the US, which accounted for 1.4% of the entire economy in 2022, with China in second position with a direct impact on GDP of 0.89%, and EU in third.

Figure 4: Incidence of the Data Economy on GDP (Only direct impacts), by geographical area



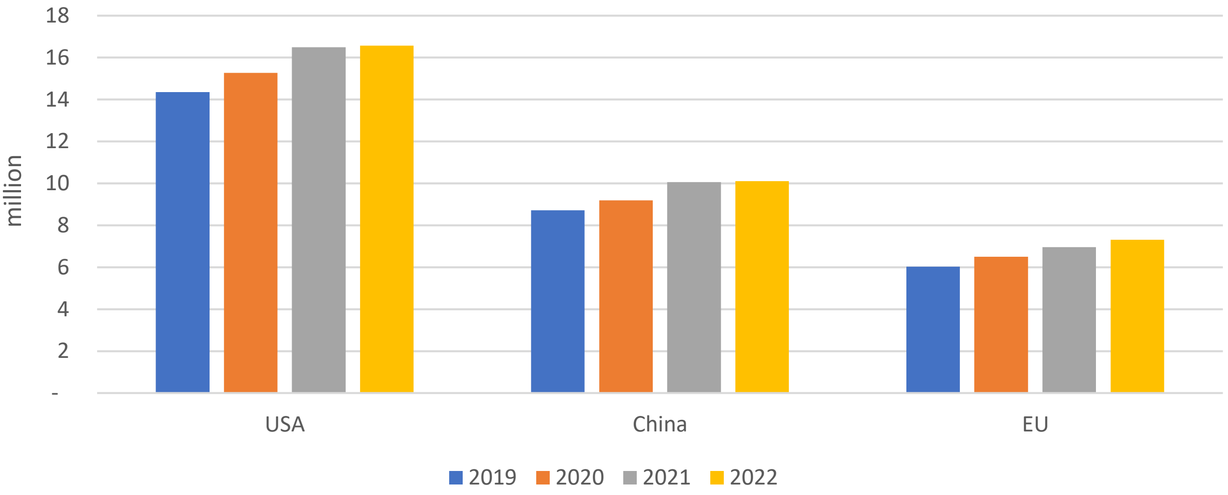
Source: IDC, European DATA Market Study 2021–2023 (Second Report, February 2023)

Referring to **data professionals** divided by geographic area, it is useful to obtain a complete frame of reference. Data professionals are "workers who collect, store, manage, and/or analyse, interpret,

[61] Specifically, direct impact refers to the "initial and immediate effects generated by the data supplier companies. The quantitative direct impacts will then be measured as the value of revenues from data products and services sold, i.e., the value of the data companies' revenues". Source: Idibem

and visualise data as their primary activity or as a relevant part of their activity. Data professionals must be proficient with the use of structured and unstructured data, should be able to work with a huge amount of data, and should be familiar with emerging database technologies"[62]. Figure 5 shows that the **US is in the lead once again, with over double the number of professionals in this field compared to the EU, and also significantly surpassing China**.

Figure 5: Number of Data Professionals, by geographical area



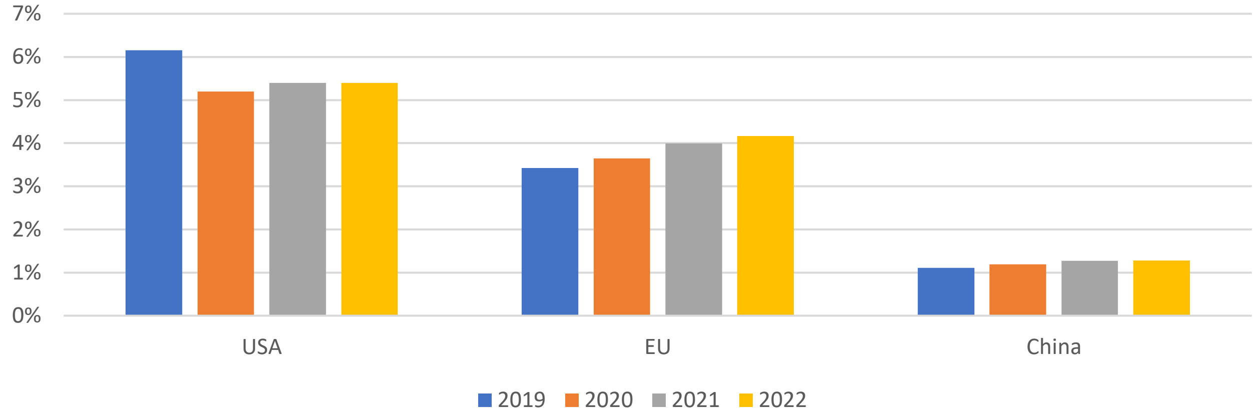
Source: IDC, European DATA Market Study 2021–2023 (Second Report, February 2023)

Fig. 6 shows the **data professional employment share**. Although there has been a small increase in the number of available data professionals, it is not significant enough to be noticeable especially between 2021 and 2022. The proportion of resources held by China and the US has remained constant compared to the share of 2021 (1.3% and 5.4%, respectively), while the **EU27 recorded an increase of 0.2%.**

Reasoning in absolute values, especially in relation to China, it can be understood how the EU must speed up its training and the inclusion in organizations of figures specialized in data management and analysis. In fact, if Europe does not respond quickly, it could in a short time fall behind in terms of technological advancement on this front compared to the other geographical areas analyzed.

[62] Ibidem

Figure 6: Data professional employment share (% Total Employment), by geographical area



Source: IDC, European DATA Market Study 2021–2023 (Second Report, February 2023)

3.3 The data economy in the EU Member States: state of the art and future projections

As already reported in the previous paragraph, the value of the data market in the European Union had reached €72,963 million by 2022, a growth of 12.6% over 2021. **Among Member States, Germany had the largest share of the Data Market in 2022, with a value of € 20,351 million** (+13.1% on 2021). There followed France and Italy, with a data market value of € 12,300 million (+14%) and € 6,886 million (+12.2%), respectively. The top five Member States (Germany, France, Italy, the Netherlands and Spain) accounted for more than 68% of the EU data market. (Fig. 7).

Focusing on industries, **Finance is the largest sector for data,** but it does not make the most substantial contribution to overall data market growth. Public Administration and Construction, on the other hand, show the greatest growth in the period 2021-2022, +41.9% and +34.9% respectively. According to the latest forecast, the EU data market will reach € 116 billion by 2030 (baseline scenario[63]). More specifically, the European data market will grow by more than € 20 billion between 2025 and 2030 and amongst the top countries contributing to this growth we find, in addition to Germany, also Spain (7.9%) and Italy (5.9%).

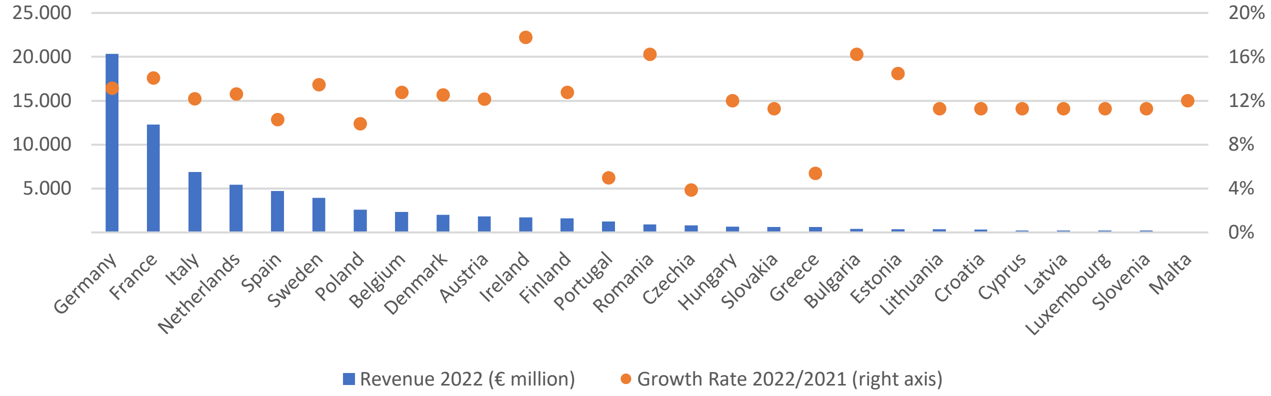
The positive trend in the data market growth is also confirmed by the **Data Economy[64] value, that reached the threshold of € 500 billion in 2022 for the EU** with an increase of 8.9% over the previous year. Moreover, **the share of overall impacts on GDP in the EU ranged from 3.7% in 2021 to 3.9% in 2022.** The IDC expects that in 2025 the data economy for the EU, will reach € 640 billion, with a

[63] Baseline scenario: Europe makes progress in the development of data infrastructures and digital resources, plays a strong role in shaping global digital governance rules building on GDPR but does not quite dominate AI-led developments.

[64] The data economy measures the overall impact of the data market on the economy as a whole. It involves the generation, collection, storage, processing, distribution, analysis, elaboration, delivery, and exploitation of data enabled by digital technologies

share on GDP of 4.8%. Finally, in 2030, the data economy for the EU is expected to remain slightly below the € 1 trillion threshold, with a 5.5% 2025–2030 CAGR and a share on GDP of 5.7%[65].

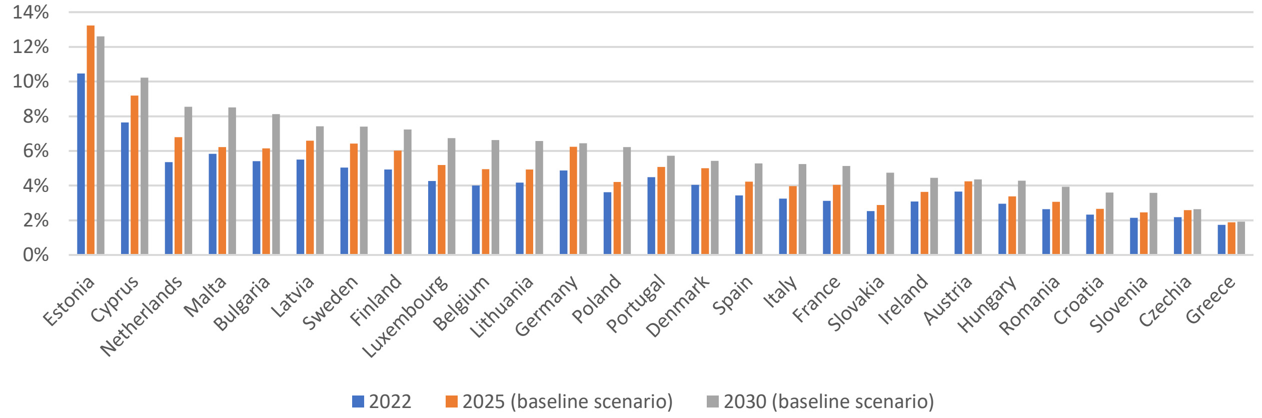
Figure 7: European Data Market, by Member State



Source: IDC, European DATA Market Study 2021–2023 (Second Report, February 2023)

The country with the largest data economy impact on GDP by 2030, according to the estimates, will be Estonia (12.6%), followed by Cyprus and the Netherlands (10.2% and 8.5%, respectively), whereas Greece will remain the least affected country (1.9%) (Fig. 8).

Figure 8: Data Economy as a % of GDP, by Member State

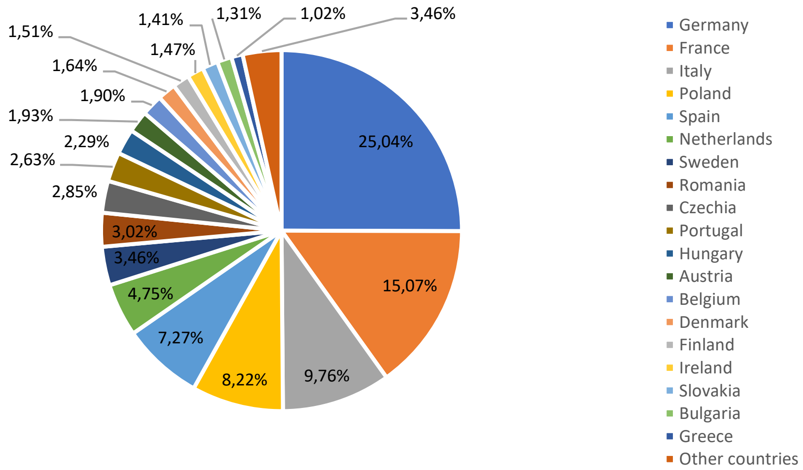


Source: IDC, European DATA Market Study 2021–2023 (Second Report, February 2023)

In order to use and exploit the progressively increasing amount of data being produced, data professionals are needed. **In 2022, there were more than 7 million data professionals in the EU, with 50% concentrated in three Member States (Germany, France and Italy)** (Fig. 9).

[65] https://digital-strategy.ec.europa.eu/en/library/results-new-european-data-market-study-2021-2023

Figure 9: Distribution of data professionals across the EU (2022)



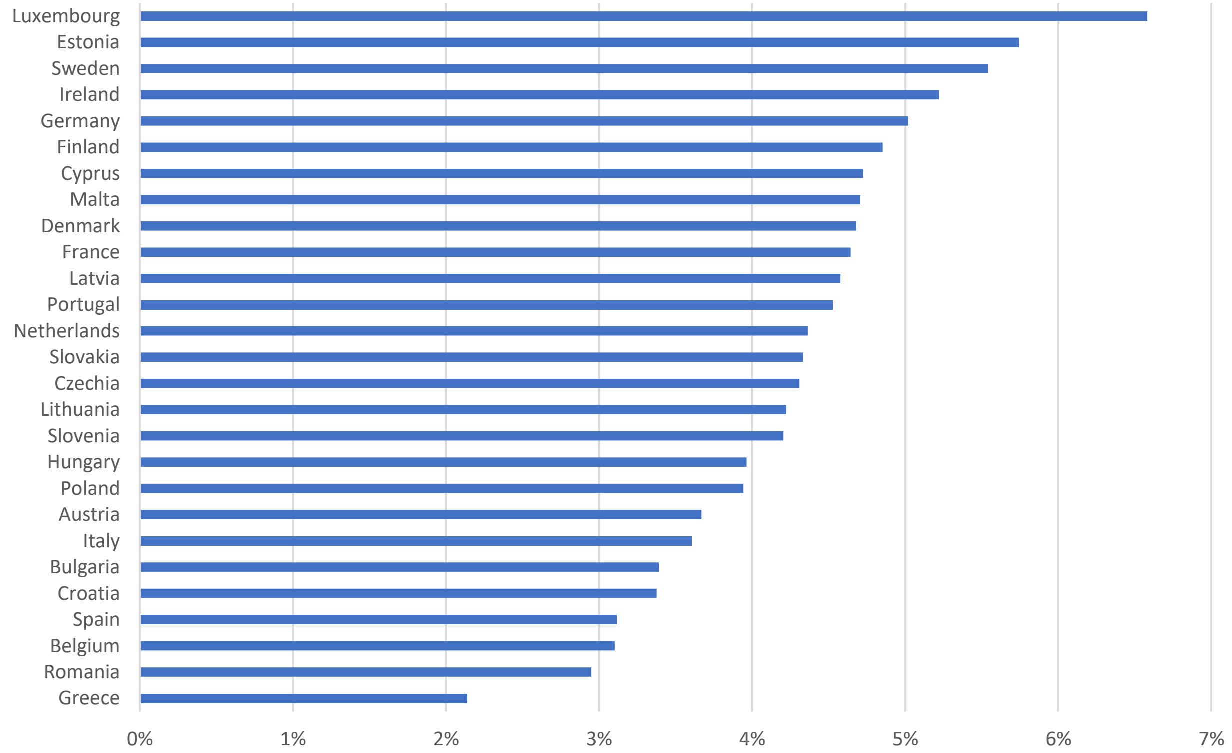
Source: I-Com elaboration on European DATA Market Study 2021–2023 (IDC 2023)

Data professionals represent 4.2% of the total employment in the EU. This share varies significantly by country, from 6.6% in Luxembourg to 2.1% in Greece (Fig. 10). In Spain and Italy, the share of data professionals in total employment is lower than the European average, i.e., 3.1% and 3.6% respectively. Instead, in Portugal, it meets the average (4.5%). According to the forecasts for 2030 (baseline scenario), the country where the number of data professionals are expected to increase the most are Malta with a CAGR of 5.6% in the period 2025-2030, followed by Slovakia (4.6%) and Portugal (4.3%).

By industry, the top three industries that account for more than half (51%) of data professionals are Professional Services, Retail and Wholesale and Information & Communication.

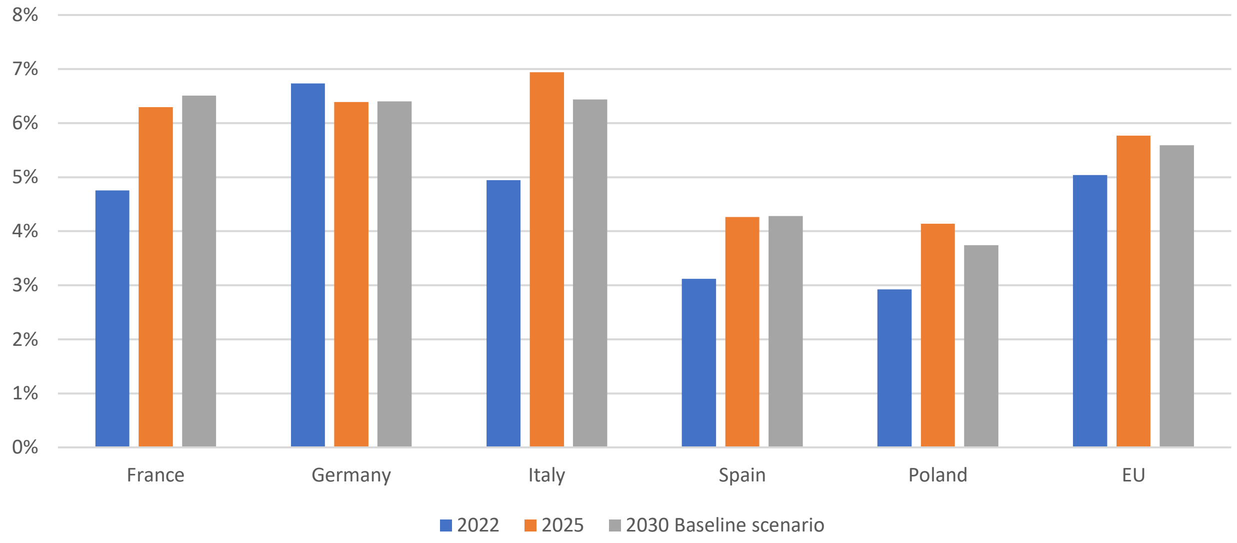
The lack of adequate skills risks becoming an important barrier to development in the data industry and the adoption of data-driven innovation in the European Union. According to the IDC study, the skills gap for data professionals is growing rapidly, and will expand even more in the 2022–2025 period. Therefore, there continues to be an imbalance between the supply and demand of data skills in Europe. **In 2022, the skills gap of data professionals was estimated at 368,000 (corresponding to 5% of total demand),and will reach 552,000 by 2030** in the baseline scenario (5.6% of total demand). France, Germany, Italy, Spain and Poland– the leading countries in terms of data professionals – show a mid-size gap in the scenario to 2030, as the positive trends of supply is not keeping up with the strong demand growth. Therefore, in France, Italy, Spain and Poland, the number of unfilled positions is expected to climb to 6.5%, 6.4%, 4.3%, 3.7%, respectively, in 2030. **Only in Germany is the skills gap expected to decline**, from 6.7% in 2022 to 6.4% in 2030 (Fig.11).

Figure 10: Share of data professionals out of total employment, by Member State (2022)



Source: IDC, European DATA Market Study 2021–2023 (Second Report, February 2023).

Figure 11: Data professional skills gap in the Big Five EU countries



Source: IDC, European DATA Market Study 2021–2023 (Second Report, February 2023)

3.4 Data-economy Index to measure Member States' performance

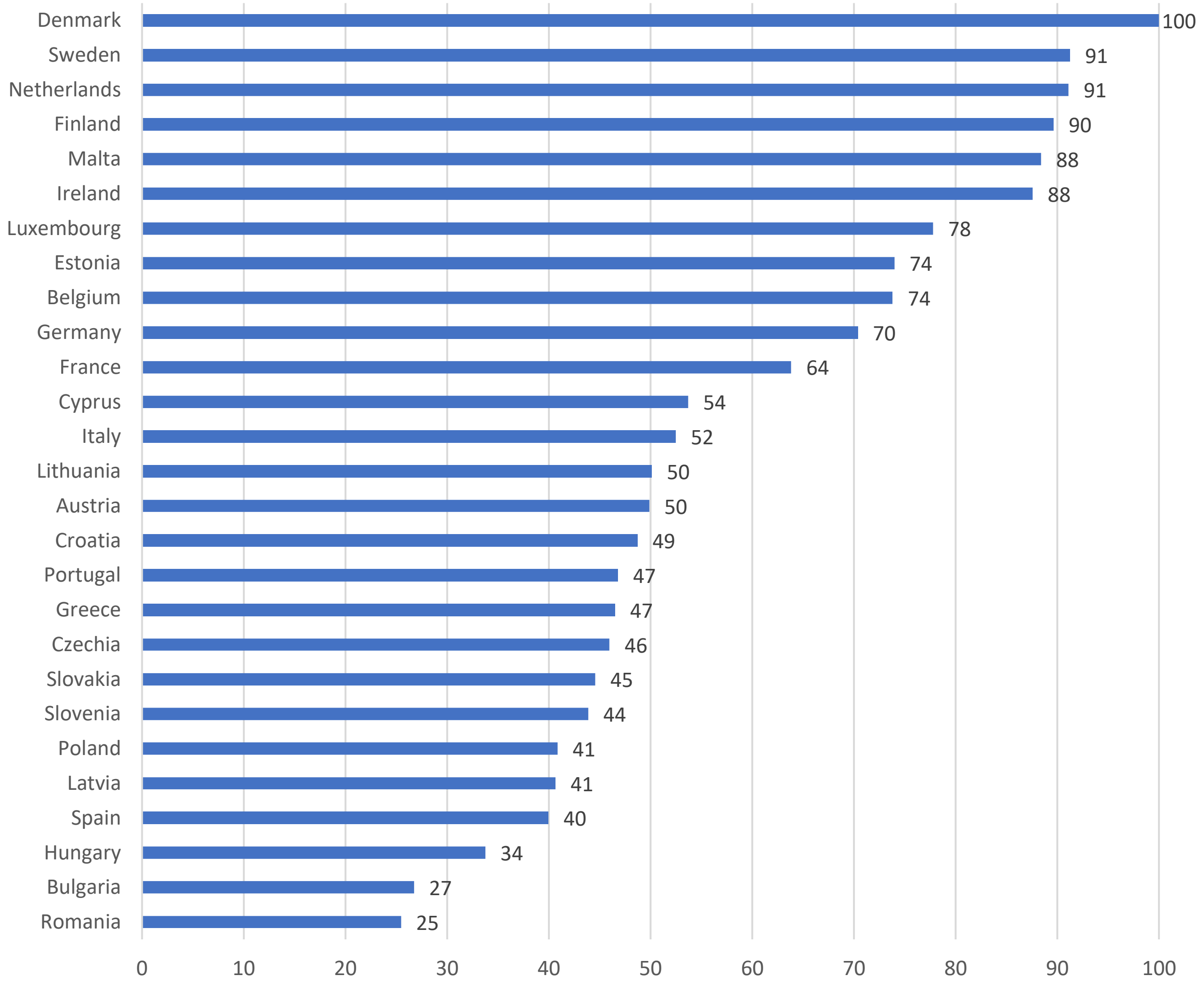
With the aim of measuring the performance of European countries in the implementation of data driven innovation, I-Com developed a synthetic index that takes into account some variables related to the data economy in the various Member States, such as:

- share of data supplier companies out of total number of companies by each country;
- share of data user companies out of total number of companies by each country;
- share of data professionals out of total employment;
- share of data market (per capita value);
- share of enterprises analyzing big data internally from any data source or externally out of total enterprises (% of total enterprises);
- share of enterprises using cloud computing services out of total enterprises (% of total enterprises).

Each listed variable will be appropriately weighted, and an average of the variables will be calculated for each country. The values obtained will be normalized with respect to the country "best performer" to establish a ranking from 0 to 100.

On the top of the rankings is Denmark with a score of 100, followed by Sweden, the Netherlands and Finland with scores of 91, 91, 90 respectively (Fig. 12). These countries, despite being small in terms of size compared to others, show a good "data ecosystem" and have enterprises that perform particularly well in terms of Big Data and the use of enabling technologies such as cloud computing. **At the bottom of the ranking, we find the countries of Eastern Europe (Romania, Bulgaria, Hungary) and Spain**, where the paradigm of data driven innovation looks still little implemented.

Figure 12: I-Com index on data economy development in the EU countries

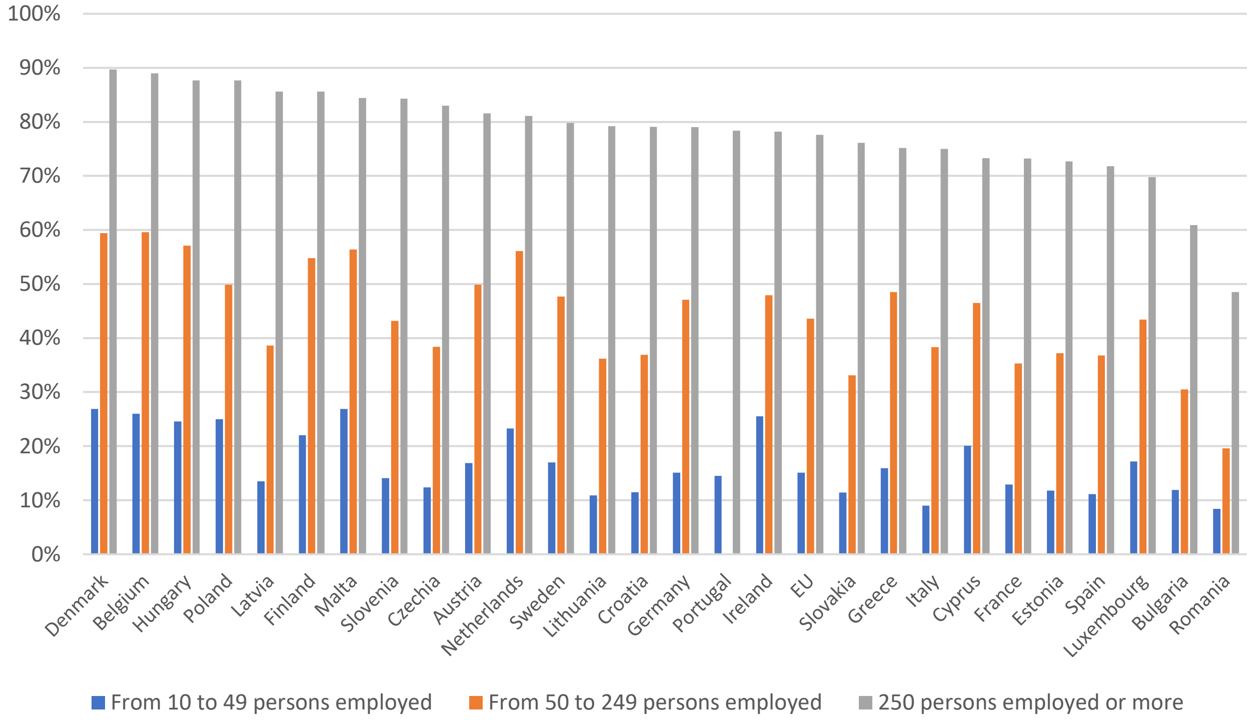


Source: I-Com elaboration on IDC and Eurostat data

3.5 The role of SMEs and skill adequacy in the Data Economy

As previously stated, data management is becoming a crucial development factor for organizations, and SMEs are no exception. Unfortunately, however, **SME companies are not often equipped with an adequate set of skills to exploit the important opportunities that can arise from data analysis**. To understand how far behind SMEs are compared to large companies regarding ICT skills, we need only look at the latest data published by Eurostat on ICT specialists. I**n 2022, nearly 80% of EU enterprises with more than 250 employees used ICT specialists**, as opposed to those with between 50 and 249 employees where this percentage is halved. **For small enterprises, this data turns out to be even lower, amounting to 15 %** (Fig. 13).

Figure 13: Enterprises in EU that employ ICT specialists, by size class of enterprise (2022)

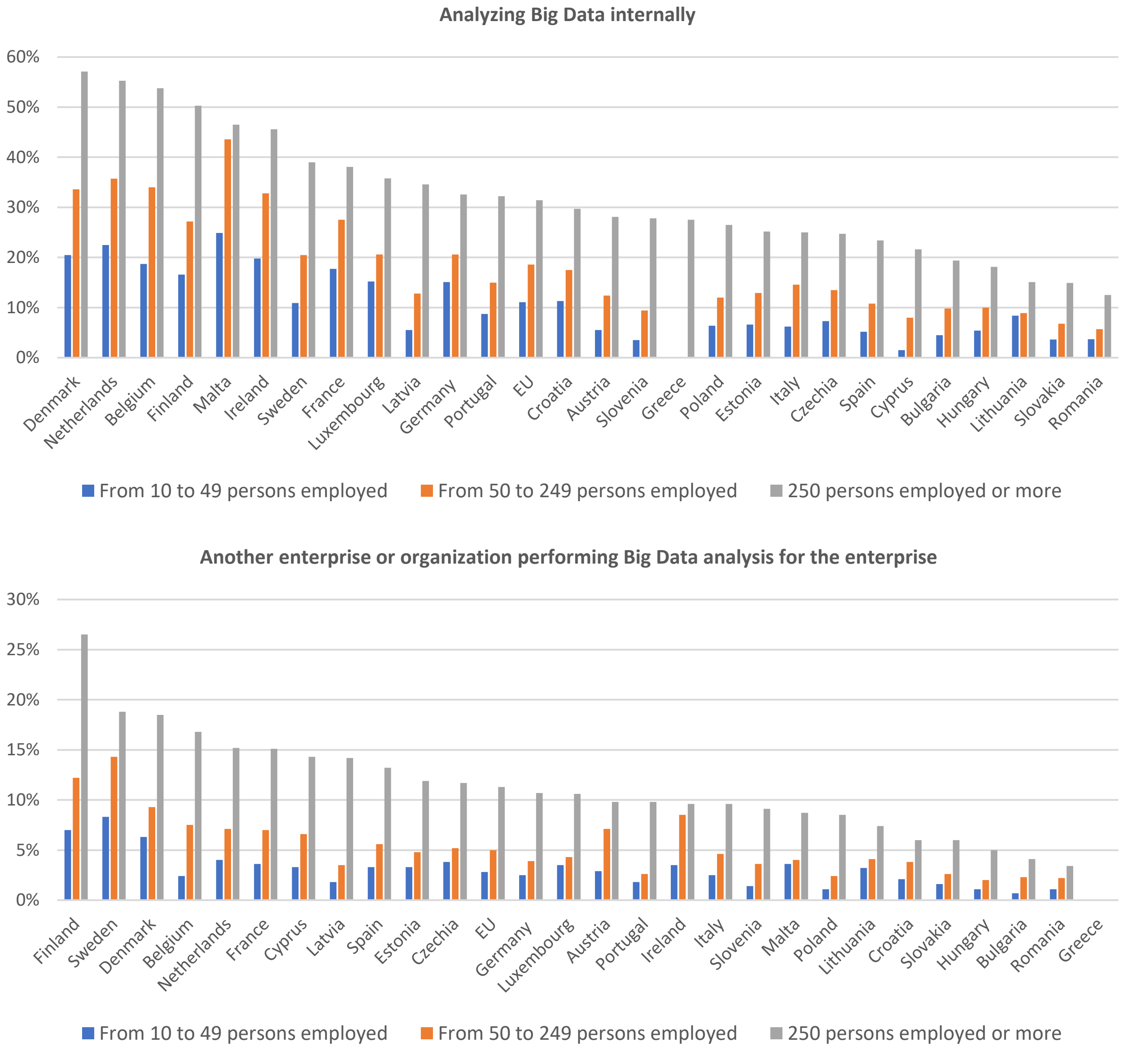


Source: Eurostat

To create value from data, it is necessary to aggregate data or data insights from different applications, locations or external data spaces. Fig. 14 illustrates the percentage of companies conducting Big Data analysis, showing the internal and external performance, respectively. **About one third of enterprises with over 250 employees perform Bbig Data analysis internally, while more than 10% outsource it to other companies or organizations. However, these percentages decrease for small and medium-sized enterprises - for companies with 40 to 249 employees, roughly 19% conduct internal analyses and only 5% rely on external analysis.**

There could be several reasons why small enterprises do not perform Big Data analysis. One possibility is that they may lack the necessary resources, such as funding, technology infrastructure, and skilled personnel, to carry out such analyses. Small enterprises may also have limited data sets, which may not justify the investment in Big Data analysis. Additionally, small enterprises may not see it as a priority compared to other pressing business needs. Another reason could be a lack of awareness or understanding of the potential benefits it may offer their business.

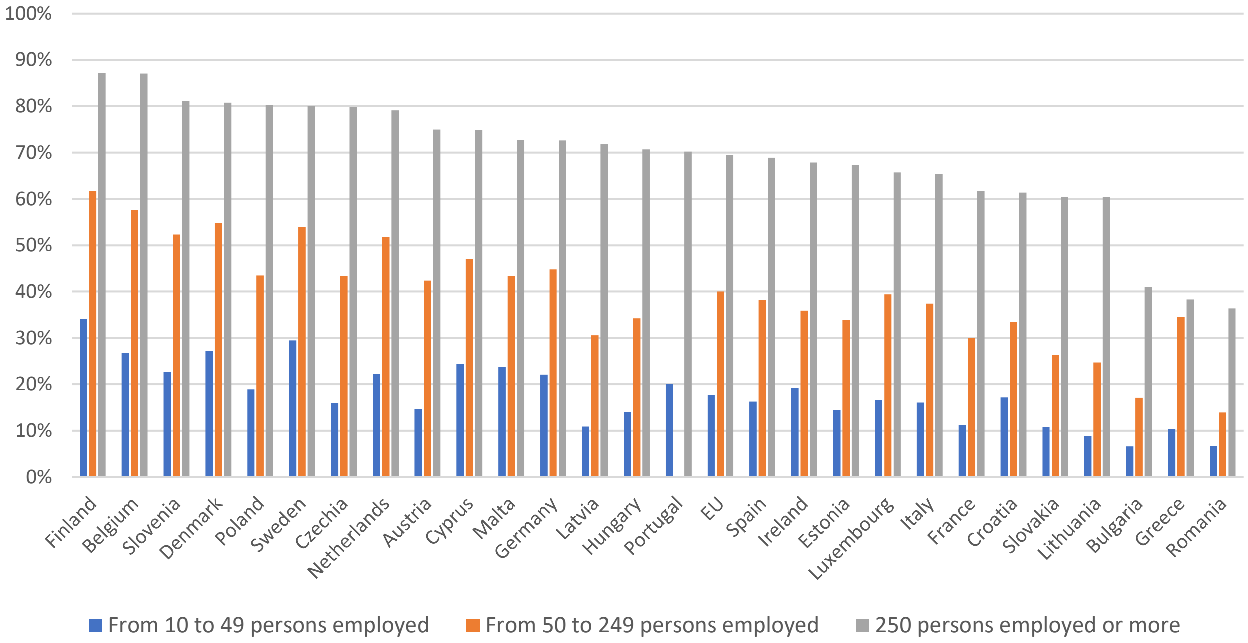
Figure 14: Big data analysis in EU, by size class of enterprise (2020)



Source: Eurostat

The data presented in Figure 15 indicates the proportion of enterprises that provided training programs to enhance their employees' proficiency in ICT skills. This representation aligns with the findings of the previous analysis where **large corporations tend to be better positioned than small businesses to acquire expertise in the field of data economy**. According to the data, most large enterprises (70%), have provided training opportunities related to Information and Communication Technology (ICT) skills. Conversely, less than half of medium-sized enterprises provided such training opportunities and for small companies, the percentage was even lower than 20%.

Figure 15: Enterprises in EU that provided training to develop/upgrade ICT skills of their personnel, by size class of enterprise (2022)



Source: Eurostat

The data shown in the above figures highlights a clear **delay of SMEs both in terms of the endowment of personnel specialized in ICT and in the digital training of total employees.** This factor is inevitably reflected in the ability of SMEs to seize the business opportunities related to the exploitation of data. **As the graphs on the use of Big Data show, only 11.1% of EU companies with 10 to 49 employees and 18.6% of those with 50 to 250 employees analyze their data internally.** Despite this, the share of companies that use external data analysis services is even lower. Adding up the percentages, in fact, we see that **only 13.9% of companies with 10 to 50 employees and 23.6% of those between 50 and 250 use Big Data in some way**. From this, we can deduce that most SMEs probably not only do not collect and analyze Big Data internally, but do not use it at all. Therefore, there is a real risk that the lack of skills in SMEs affects not only the ability to analyze data, but also the ability to understand the importance that such data might have on business performance.

Chapter 4: Digital revolution and the health sector focusing on the Southern European countries

4.1 Introduction

Our chapter aims to describe the **digital transition of the health sector and the secondary usage of health data in the light of the European Health Data Space (EHDS), focusing on Southern Europe (Greece, Italy, Portugal, Spain).**

In May 2022, the European Commission commenced the European Health Data Space (EHDS) planning to improve the provided healthcare. More specifically, the EHDS could enhance the citizens digital access to their private health information, support access of medical professionals to health data, assist academia, regulatory activity and policy making by providing non-identifiable health data while facilitating complete adherence to the strict data privacy standards set by the EU.

European Commission expects a variety of benefits not only in economic terms but also with respect to several stakeholders. **Improved access and transfer of health data in the healthcare sector could save 5.5 billion € for the EU over ten years in combination with € 5.4 billion that could be saved for the EU from optimal use of health data by the research and innovation community and also by the policymakers.** Furthermore, the potential growth of digital health care is estimated between 20-30%[66]. Another critical benefit is the boost of investments in Research and Development (R&D) by facilitating access to Real World Evidence.

Apart from the economic aspect, EU citizens will gain immediate, costless access to their health data while their security and privacy are ensured, similar to health professionals decreasing the relative administrative burden. Effective access to health data would significantly benefit the research community, regulation and policymaking since data will be provided transparent and cost-efficiently. The health industry could be benefited substantially also by data standardization since the non-identifiable digital health data could provide significant insights for fostering innovative activity[67].

Though the benefits of the EHDS could be significant for healthcare policy and innovation, certain challenges also emerge. Health information is the most sensitive type of data, and privacy ensuring should always be a top priority. Therefore, cybersecurity, storage and connection with other information are issues of great concern since the EHDS requires interoperability among many different data sources. Unidentified provision of data for research and other policy issues should also be a critical aspect to ensure. Transparency in data management, privacy protection and taking patient consent could increase trust and foster health digitalisation.

Next, we analyse the digital readiness of the four examined countries focusing on the health sector. We present evidence regarding their performance in the Digital Economy and Society Index (DESI) and its subdimensions, the digital health market projections, and the digital health

[66] European Commission. (2022a). Factsheet - European Health Data Space (EHDS. Retrieved May 11, 2023, Available at https://health.ec.europa.eu/latest-updates/factsheet-european-health-data-space-ehds-2022-05-03_en

[67] Ibid.

performance of the country using indexes available from Future Proofing Healthcare Index. Also, we utilise the findings of the report published by the Open Data Institute (ODI) in 2021[68] to evaluate the performance and readiness at the policy level of Italy, Portugal, Spain and Greece on the six best practice categories, including infrastructure, capabilities development, healthcare innovation, equity, ethics, and public engagement. **Overall, Greece is characterised as less prepared since poorer policy quality and less advanced execution stages are present. On the other hand, Italy, Portugal, and Spain are leading the way since their quality of policy is superior, and the implementation stage is further along.**

4.2 Digital readiness of the health sector focusing on secondary usage of health data

4.2.1 Spain

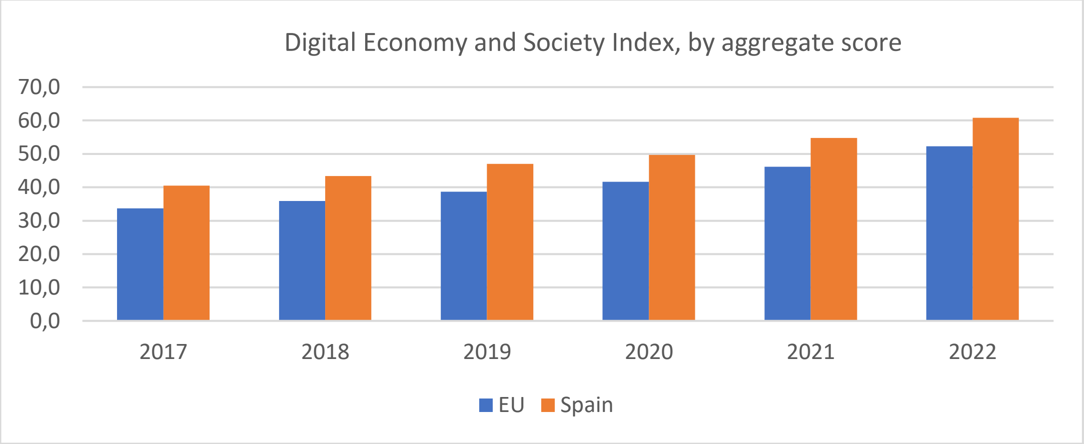
In total, **Spain is strong in the field of digital transformation, and its progress is evident since the country ranks 7th in the 2022 Digital Economy and Society Index (DESI) index (11th in 2021)**. Spain is one of the leading countries in terms of connectivity, and its strong advantage is in a fixed, very high-capacity network (VHCN) with a coverage of 94% (compared to the EU average of 70%). In the human capital dimension, the country ranked 10th in the EU (EU average 45.7%), and 38% of individuals present above basic digital skills, while the EU average was 26%. Integration of digital technology is the least developed indicator in the country but still is slightly higher (38.5) than the EU average (36.1).

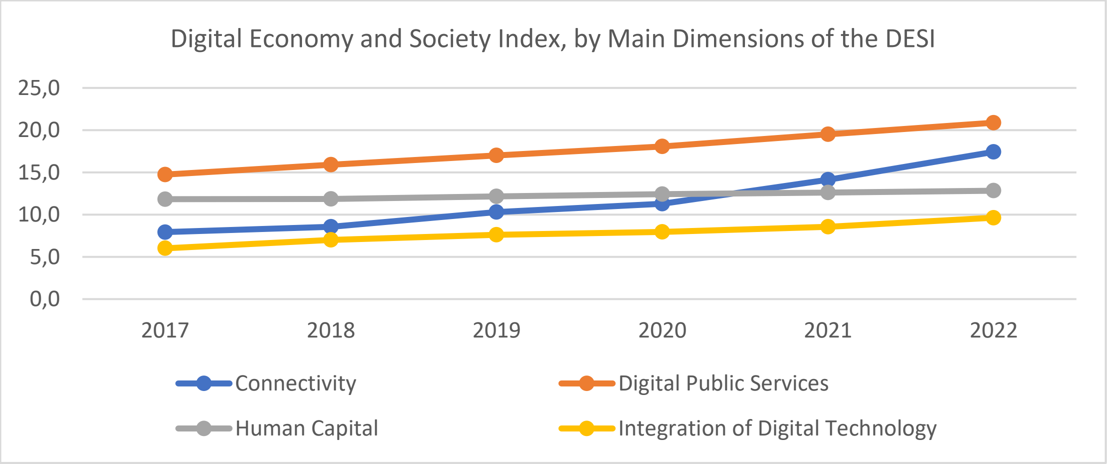
Digital Public Services is a strong asset of Spain; it is the DESI indicator that the country excels with a score equal to 83.5, ranking 5th among the EU Member States**. The country dynamically promotes new digital services, among others, in the health sector**. Responsibility for healthcare provision is shared among the National Health System (Sistema Nacional de Salud) at a central level but also by the autonomous communities. To strengthen the information exchange at the regional and central levels, the facilitation of interoperable health systems is promoted.

According to Statista, the revenue in the Digital Health market is expected to be €1.90 billion in 2023 (revenue change by segment 16.9% in 2023) with an annual growth rate (CAGR 2023-2027) of 6.48%, leading in a projected market volume of €2.44 billion by 2027. The definition of the Digital Health market includes, among others, mobile health apps, connected wearable devices, and telemedicine, and it is divided into two segments Digital Fitness & Well-Being and eHealth.

[68] Boyd, M., Zimeta, M., Tennison, J., & Alassow, M. (2021). Secondary use of health data in Europe. Open Data Institute, Roche.

Figure 16 Comparison of Spain's digital performance to EU in the DESI 2022





Source: European Commission, Digital Scoreboard

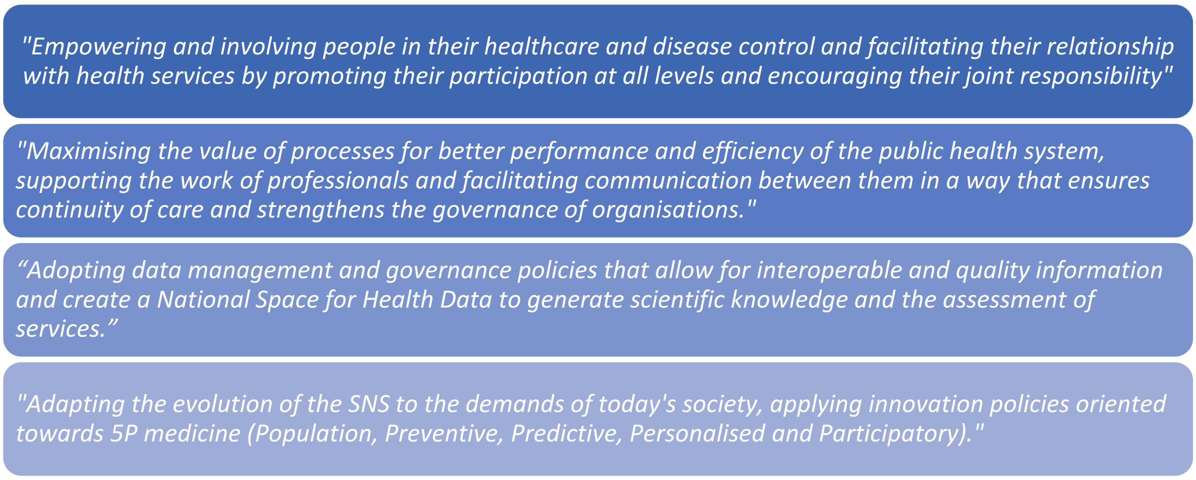
According to a report published in February 2023 by the General Secretariat for Digital Health, Information and Innovation for the SNS (National Health System)[69], a specific Digital Health Strategy will be developed in the country for the 2021 – 2026 period. It aims to facilitate an environment where the public sector's digital health transformation efforts could flourish by interacting with all stakeholders involved, and it provides governance and monitoring mechanisms. The strategy focuses on strengthening the public health system through digitalisation aimed at citizens, health professionals, health service providers and other relevant stakeholders. The specific strategic objectives, as mentioned in the report, are presented in Shape 1. The policy is based on three main lines of actions that foster the digital transition of the Spanish health sector a) the development of

[69] Available here https://www.sanidad.gob.es/ciudadanos/pdf/Digital_Health_Strategy.pdf

digital health services focusing on equity, b) the generalisation of the interoperability of health information and c) the strengthening of health data analytics.

In addition, ten intervention areas are defined in the strategy report, where the effect of digitalisation is expected to be notably positive, which are described in Shape 2. The strategy is directly associated with the "Recovery Assistance for Cohesion and the Territories of Europe (REACT-EU)" and the "Recovery and Resilience Mechanism" with the potential to participate in other EU programmes.

Shape 1 Strategic objectives of Spanish Digital Health Strategy - National Health System (SNS), by the General Secretariat for Digital Health, Information and Innovation for the National Health System



"Empowering and involving people in their healthcare and disease control and facilitating their relationship with health services by promoting their participation at all levels and encouraging their joint responsibility"

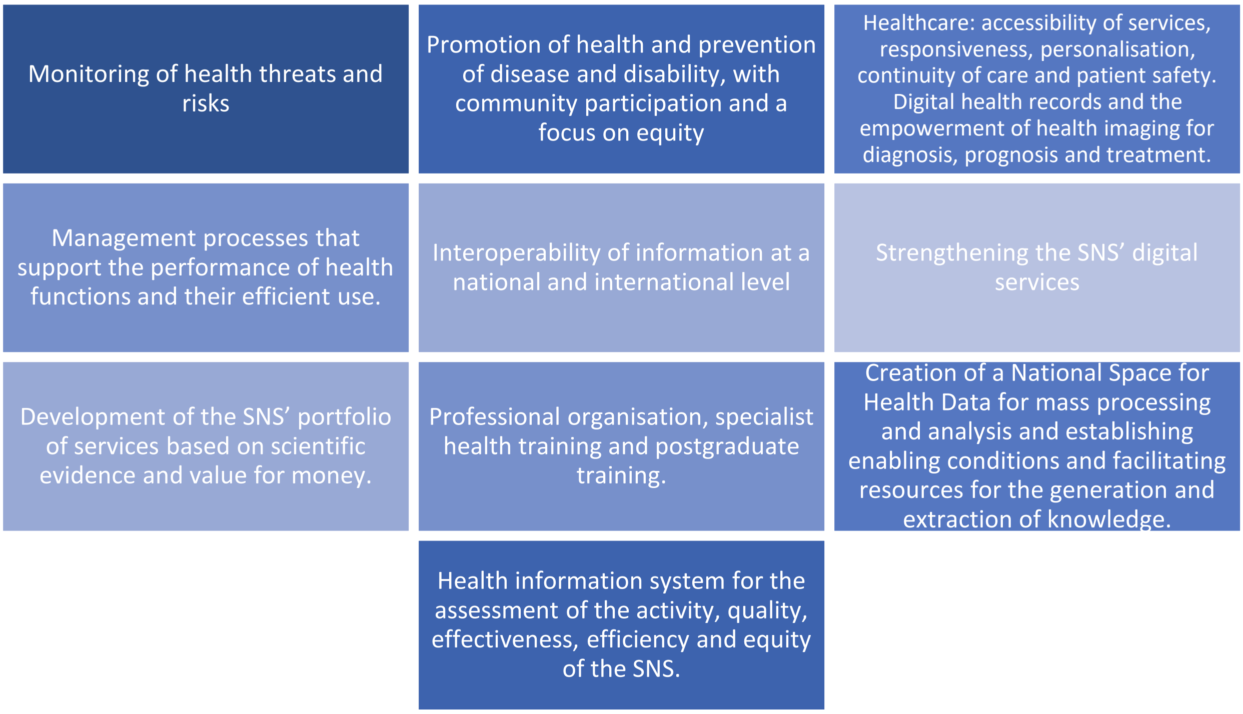
"Maximising the value of processes for better performance and efficiency of the public health system, supporting the work of professionals and facilitating communication between them in a way that ensures continuity of care and strengthens the governance of organisations."

"Adopting data management and governance policies that allow for interoperable and quality information and create a National Space for Health Data to generate scientific knowledge and the assessment of services."

"Adapting the evolution of the SNS to the demands of today's society, applying innovation policies oriented towards 5P medicine (Population, Preventive, Predictive, Personalised and Participatory)."

Source: General Secretariat for Digital Health, Information and Innovation for the SNS, Spanish Ministry of Health (Ministerio de Sanidad)

Shape 2 Ten areas of intervention of Spanish Digital Health Strategy - National Health System (SNS), by the General Secretariat for Digital Health, Information and Innovation for the National Health System



Monitoring of health threats and risks

Promotion of health and prevention of disease and disability, with community participation and a focus on equity

Healthcare: accessibility of services, responsiveness, personalisation, continuity of care and patient safety. Digital health records and the empowerment of health imaging for diagnosis, prognosis and treatment.

Management processes that support the performance of health functions and their efficient use.

Interoperability of information at a national and international level

Strengthening the SNS’ digital services

Development of the SNS’ portfolio of services based on scientific evidence and value for money.

Professional organisation, specialist health training and postgraduate training.

Creation of a National Space for Health Data for mass processing and analysis and establishing enabling conditions and facilitating resources for the generation and extraction of knowledge.

Health information system for the assessment of the activity, quality, effectiveness, efficiency and equity of the SNS.

Source: General Secretariat for Digital Health, Information and Innovation for the SNS, Spanish Ministry of Health (Ministerio de Sanidad)

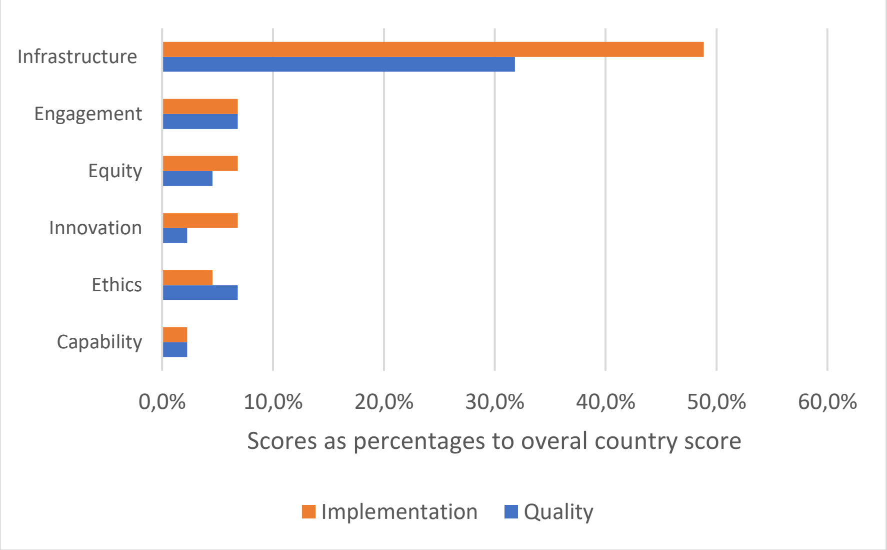
Specifically, **regarding the secondary use of health data, Boyd et al.[70] indicate that the policy stage in Spain is vaguer since there is no relative strategy specified**. In Europe, Spain belongs to the leaders’ group in country policy rankings, and in 17, the country’s score is analysed. Leaders group, as the report suggests, a) acknowledging the importance of secondary use of health data for innovation, individualized treatment, and enhanced diagnostics, b) enhancing the ecosystems and infrastructure for health data and data reuse, and c) utilizing real-world information in health systems.

The strong assets of Spain, according to Future Proofing Health Index, in the patient rights to access data in 2018, where Spain ranked first in Europe and 5th in the use of Telehealth (source of data 2015), the country was significantly behind (33rd) regarding the access to Data for Research (2019 data). Regarding the use of Electronic Health Records (EHRs) through primary, secondary and tertiary healthcare facilities, Spain positioned 7th in 2015, while the data infrastructure was lagging in 2016, in accordance with the same index.

[70] Boyd, M., Zimeta, M., Tennison, J., & Alassow, M. (2021). Secondary use of health data in Europe. Open Data Institute, Roche.

Boyd et al.[71] recognize **two main challenges** regarding the facilitation of policy framework of secondary utilisation of health data. Firstly, **implementations that are slow and stalled**. Although various frameworks, such as real-world evidence (RWE) networks and platforms, have been established, it is unclear if they are still in use. Also, important datasets and health registries are not publicly updated or provided on a regular basis. Secondly, **the potential fragmentation is a reason for concern since the secondary use of health data**, including HERs and health sector innovation efforts with secondary use of health data, is at the regional level.

Figure 17 Secondary use of health data policy, Score of Spain



Source: Boyd et al. (2021)

4.2.2 Portugal

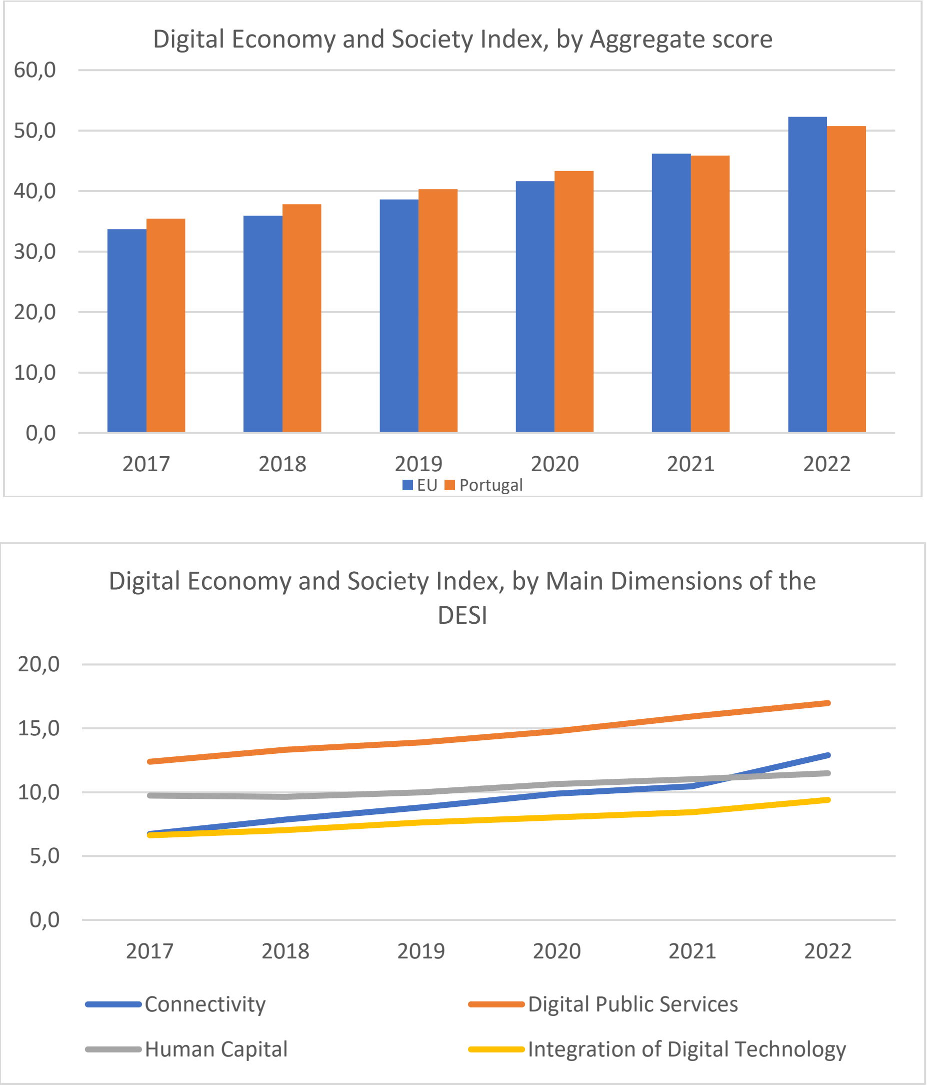
Portugal is close to the EU average (15th position) in the 2022 DESI, though its relative progress is lagging behind its peers; thus, there is room for improvement. Similarly, in terms of the human capital dimension is in line with the EU average, while 29% of individuals acquire above-basic digital skills (the EU average is equal to 26%). With regards to connectivity, the country received the 18th position among EU Member States. Strong assets of the country are the fast broadband (NGA) coverage and fixed Very High-Capacity Network (VHCN) coverage due to public and private investment during the last years[72]. In integrated digital technologies to businesses, the country performs slightly above the EU average and ranks 12th. **Digital public services is the dimension that Portugal performs best, with the indexes of Pre-filled forms and Digital public services for citizens** (score of 76 and 79 respectively) **exceeding the EU average significantly** (score of 64 and 75 accordingly) though the country is lagging in Open data with a score equal to 66% (81% in EU).

[71] Boyd, M., Zimeta, M., Tennison, J., & Alassow, M. (2021). Secondary use of health data in Europe. Open Data Institute, Roche.

[72] European Commission. (2022d). The digital economy & society index: Country profile of Portugal

Statista provides some insights regarding the market value of the digital health sector in the country. The digital health sector expected revenue in 2023 is equal to € 361.90 million, using projections, which is forecasted to follow a yearly growth rate (CAGR 2023-2027) of 6.85%, reaching a projected market volume of € 471.70 million by 2027. The largest market share is allocated to Digital Fitness & Well-Being, with € 210.70 million of total revenue in 2023.

Figure 18 Comparison of Portugal's digital performance to EU in the DESI 2022



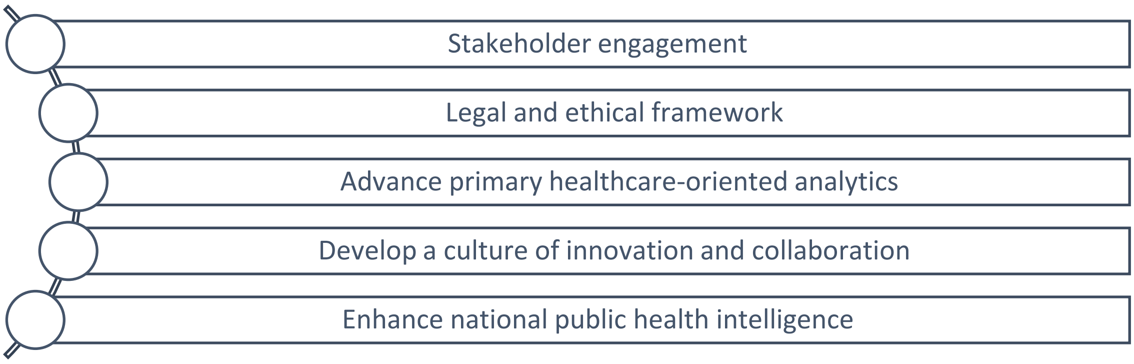
Source: European Commission, Digital Scoreboard

In the field of e-health, **Portugal's environment is quietly advanced since the country has implemented two consecutive relevant strategies, the ENESIS 2020** (ran until December 2019) **and**

the ENESIS 2022[73] (National Strategy for the Health Information Ecosystem | Estratégia Nacional para o Ecosistema de Informação da Saúde 2020- 2022). The goal of the renewed strategy was to establish the framework and conditions for the various stakeholders of the health system to contribute to its evolution. This approach extends to the entire Health System in line with the Basic Health Law, approved by Law No. 48/90 of August 24[74].

Among the initiatives of ENESIS 20-22, worthy of mention, is 'From Big Data to smart data: putting data to work for the Public's Health', which is the Data Strategy for Next Generation Portuguese National Health Service. It lays out the goals, focus areas, and guiding principles for using advanced analytics, artificial intelligence, and secondary data aiming at the enhancement of National health. The strategy conceptualized the usage of the data collected through the national health information system aiming to boost the influence of information on health policy, healthcare, and public health while ensuring accountability. To ensure a responsible and ethical digital transition of the NHS, the strategy relies on four core values a) maintaining trust through data protection and confidentiality, b) validating and assuring the data quality, c) efficiency in data management employing interoperability and integration, and d) data-driven healthcare innovation employing technology and A.I.[75]. In Figure 19, the key areas of the data strategy are described.

Figure 19 Key areas for a data-driven National Health Service in 'From Big Data to smart data: putting data to work for the Public's Health


Stakeholder engagement
Legal and ethical framework
Advance primary healthcare-oriented analytics
Develop a culture of innovation and collaboration
Enhance national public health intelligence

Source: (Pinto et al., 2019)

Future Proofing Healthcare Index ranks Portugal 14th among European countries in total. In the digital health field, the country ranked 1st in the dimension of Cross-border Data (secure and automatic transfer of patient data to transnational networks, year of data 2018). The country was positioned 16th regarding data infrastructure, 10th in patents' right access to data, 6th in the access of researchers to data and 8th in the use of EHRs. Portugal is the leading country regarding Patient

[73] https://www.digitalhealthportugal.eu/#ABOUTUS

[74] https://www.spms.min-saude.pt/enesis-2/

[75] Pinto C. S. , Martins J. P. , Martins H. (2019). FROM BIG DATA TO SMART HEALTH: PUTTING DATA TO WORK FOR THE PUBLIC´S HEALTH Data Strategy for Next Generation Portuguese National Health Service. Advanced Analytics and Intelligence Unit, Shared Services of the Ministry of Health

Portals that are used and 9th in the dimension of Telehealth. People in Portugal hesitate a lot to share their personal data since the country ranked 23rd in the Civic Participation Index.

According to Oliveira et al.[76], EHRs are used by primary healthcare providers and the majority of hospitals, and interoperability between various EHR systems has been accomplished to some extent. The Portuguese Health Data Platform (Plataforma de Dados da Saúde) includes Patient, Professional, Institutional, and International Portals in the NHS[77], and it supports various user categories and provides features for electronic prescriptions, appointments, disease-specific registrations, and data from the long-term care network, though interoperability needs improvement[78].

Boyd et al.[79] provide a national profile of Portugal regarding the progress of health data secondary use at the policy level. **The policy quality that Portugal offers is relatively high, though there is room for more progress regarding the implementation. Portugal belongs to the leading countries in their ranking**. As they highlight, the proposed health strategies frequently require more funding and increased capacities to be successful. Investment in the transition of EHRs infrastructure is limited, combined with partial training of health sector stakeholders. Also, lacking direction intended for scaling pilot projects into national health-data infrastructure is mentioned by the report. Certain challenges for fostering progress in the field include a) the potential fragmentation of the EHRs systems that could hinder interoperability, b) the implementation stage being in its first steps since strategies belong to most advance in Europe, but the execution is still in progress since further investing in infrastructure is required, c) the ecosystem capability being limited and d) lacking patient and multi-stakeholder engagement is indicated since relevant efforts are still in discussion.

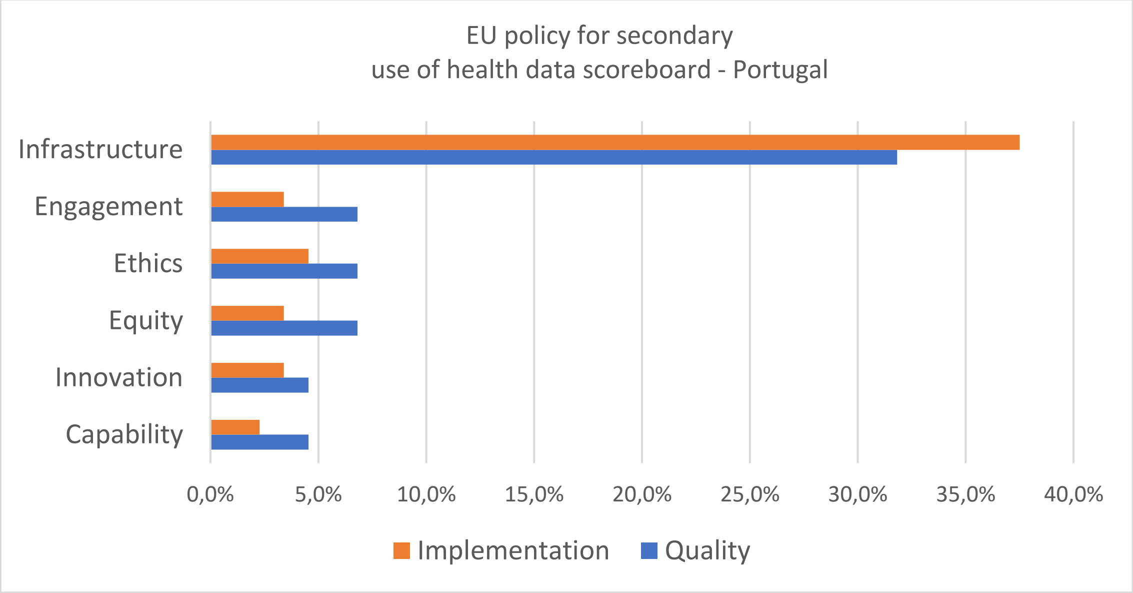
[76] Oliveira, M. D., Tavares, A. I., Vieira, A., & Pacheco, M. (2022). Sustainability and Resilience in the Portuguese Health System. Available at https://www.astrazeneca.pt/content/dam/az-pt/PDFs/PHSSR%20-%20Portugal_Relat%C3%B3rio%20Final.pdf

[77] website (www.sns.gov.pt)

[78] Supra note, 76.

[79] Boyd, M., Zimeta, M., Tennison, J., & Alassow, M. (2021). Secondary use of health data in Europe. Open Data Institute, Roche.

Figure 20 Secondary use of health data policy, Score of Portugal



Source: Boyd et al. (2021)

4.2.3 Italy

Italy is placed 18th among EU Member States in DESI 2022, though the progress through the years is significant. The establishment of a Ministry responsible for digital affairs signifies the importance of the subject to policymaking in combination with relative strategies and policy measures[80]. Italy is lagging behind in the human capital dimension of the index (25th position in EU), with 46% of individuals having at least basic digital skills, while the EU average is equal to 54%. In digital public services, the country is positioned 19th, with only 40% of internet users conducting digital public transactions, and the scores of digital public services for citizens and businesses are relatively low, though open data policies outperform the EU average (92% and 81% respectively). On the other hand, **the country is relatively strong in the connectivity dimension, ranking 7th, scoring 61.2 when the EU average is equal to 59.9**. Similarly, in the integration of digital technology by firms, the country's ranking is 8th, being an especially strong performer in the sub-dimensions of SMEs with at least a basic level of digital intensity, cloud adoption and e-Invoices issuing[81].

In the past two years, **the deployment of electronic health records was limited and regionally dispersed**. In Piano Nazionale di Ripresa e Resilienza, in the context of Next Generation EU, health data platforms and digitalisation are described as enablers of improved healthcare and healthcare governance[82]. Throughout the Italian Recovery and Resilience Plan (RRP) (€ 191.5 billion), € 1.3 billion is invested in transforming the EHRs, ensuring interoperability and portability at the regional

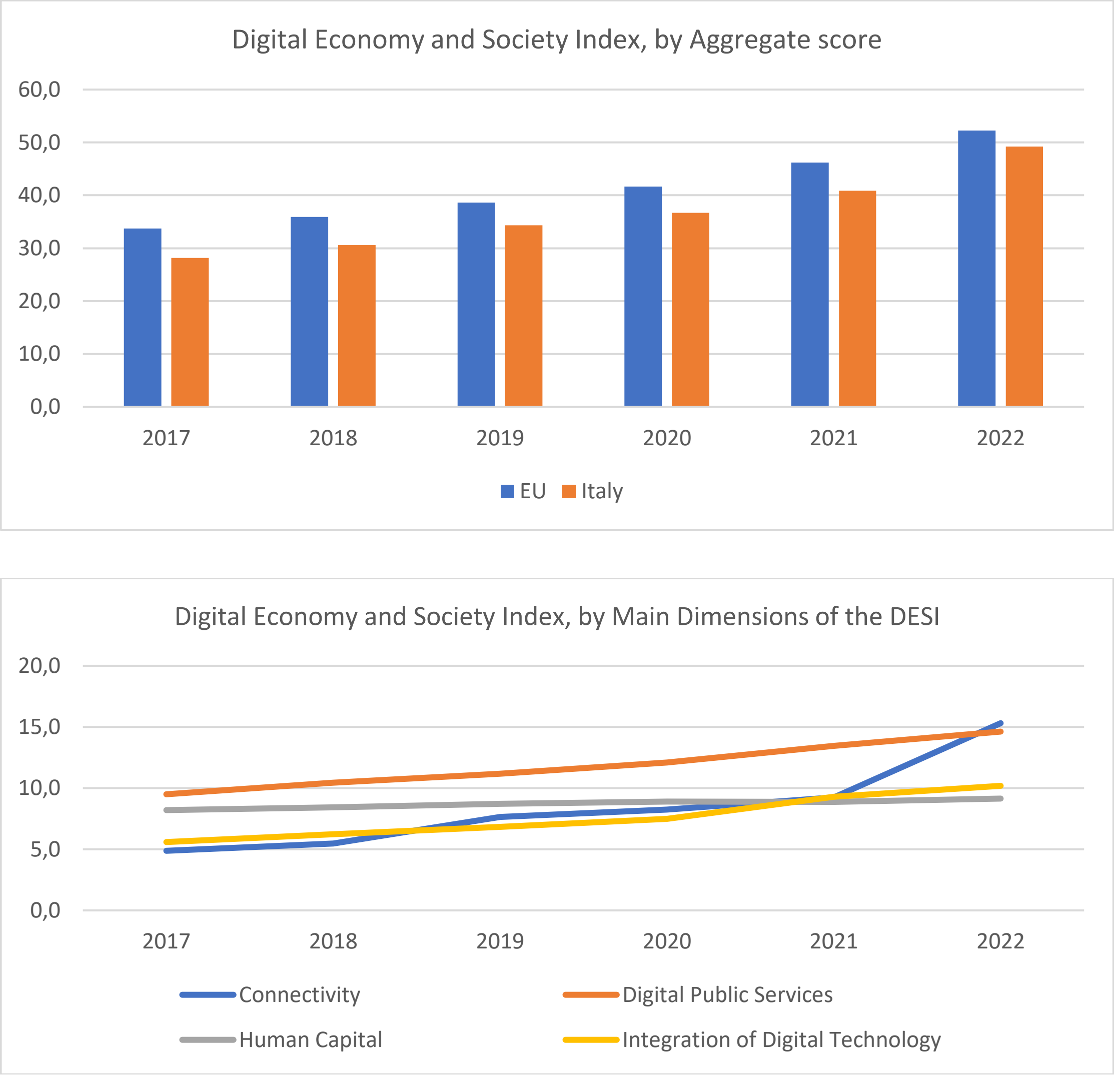
[80] European Commission. (2022c). The digital economy & society index: Country profile of Italy

[81] Ibid.

[82] Boyd, M., Zimeta, M., Tennison, J., & Alassow, M. (2021). Secondary use of health data in Europe. Open Data Institute, Roche.

level[83]. The EHRs operate in 21 regions giving access to patients to their medical history, managed at a regional level, and information can be shared with health professionals[84].
Another milestone through RRP, worthy of mention, is the **'Sanità connessa'** (Connected Healthcare facilities). **The purpose of 'Sanità Connessa' is the establishment of symmetric** connectivity (1 Gbps - 10 Gbps subject to facility type) **among 12,300 healthcare facilities, comprising management, technical support, and maintenance services for at least five years** (European Commission, 2022c).

Figure 21 Comparison of Italy's digital performance to EU in the DESI 2022



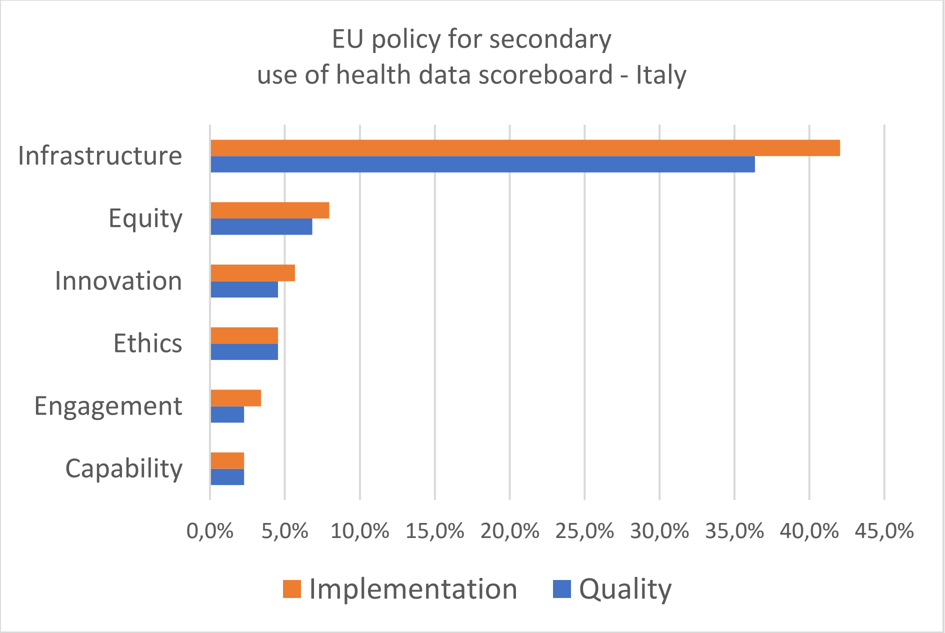
Source: European Commission, Digital Scoreboard

[83] Supra note, 80.
[84] Velametis. (2021). Adoption of eHealth in Selected European Countries (2022+). Available at https://velametis.com/2021/07/14/adoption-of-ehealth-in-selected-european-countries-2022/

The digital health sector **expected revenue in 2023 is equal to € 2.56 billion**, using projections, which is forecasted to follow a yearly growth rate (CAGR 2023-2027) of 7.57%, reaching a projected market volume of €3.43 billion by 2027. The largest market share is allocated to eHealth, with € 1.38 billion of total revenue in 2023. The forecasting statistics about the market are estimated by Statista. In Future Proofing Healthcare Index, Italy follows Portugal (15th position). Regarding health information, the country ranks 16th and more specifically, Italy is 10th in the patient right to access data (source of data 2015), similar to the patient portals index (the year 2018). However, the country leads the way, ranking 3rd in the dimension of Cross-border transfer of Data securely (year of data 2018), while access to research is relatively low since the country ranks 16th. In Telehealth, Italy positions 17th (year of data 2015) and in the utilisation of EHRs 14th (data source 2015).

Boyd et al.[85] analyse the stage of the secondary use of health data at the policy level in Italy. According to the report, **the country performs better in the dimension of implementation and relatively lower regarding the quality of the policy regime**; still, the country belongs in the leading countries group. At the end of 2018, new guidelines for the secondary use of health data for research purposes were released by the General Data Protection Authority, facilitating the relative data usage environment (Boyd et al., 2021). As any country, Italy needs to address certain policy challenges. Regional fragmentation of the healthcare system is a concern for health data initiatives at the national level since data might differ in many aspects, especially in their quality. Also, the strictness of the interpretation of local data privacy laws regarding the secondary usage of health data could be another issue to examine (Boyd et al., 2021).

Figure 22 Secondary use of health data policy, Score of Italy



Source: Boyd et al. (2021)

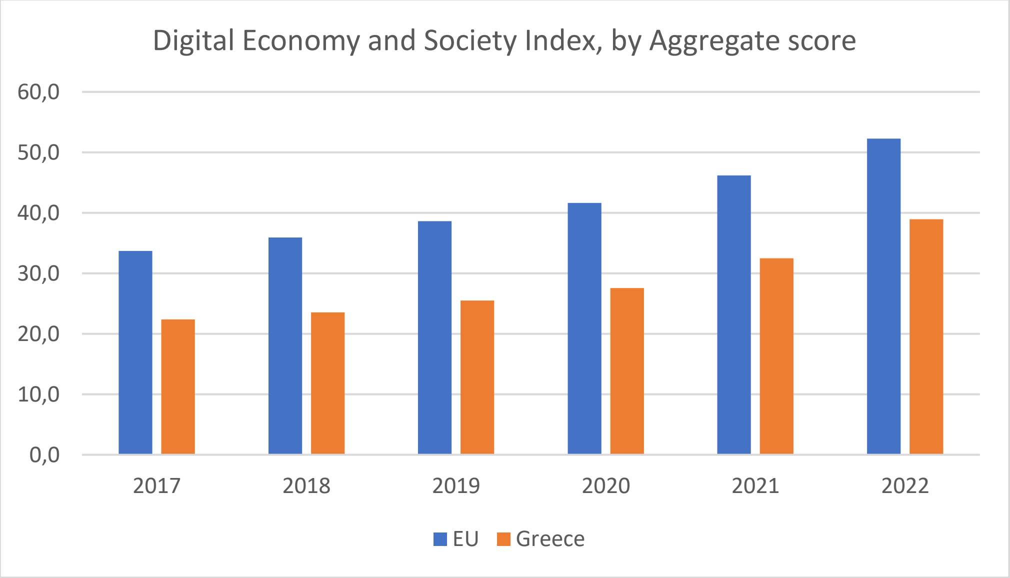
[85] Boyd, M., Zimeta, M., Tennison, J., & Alassow, M. (2021). Secondary use of health data in Europe. Open Data Institute, Roche.

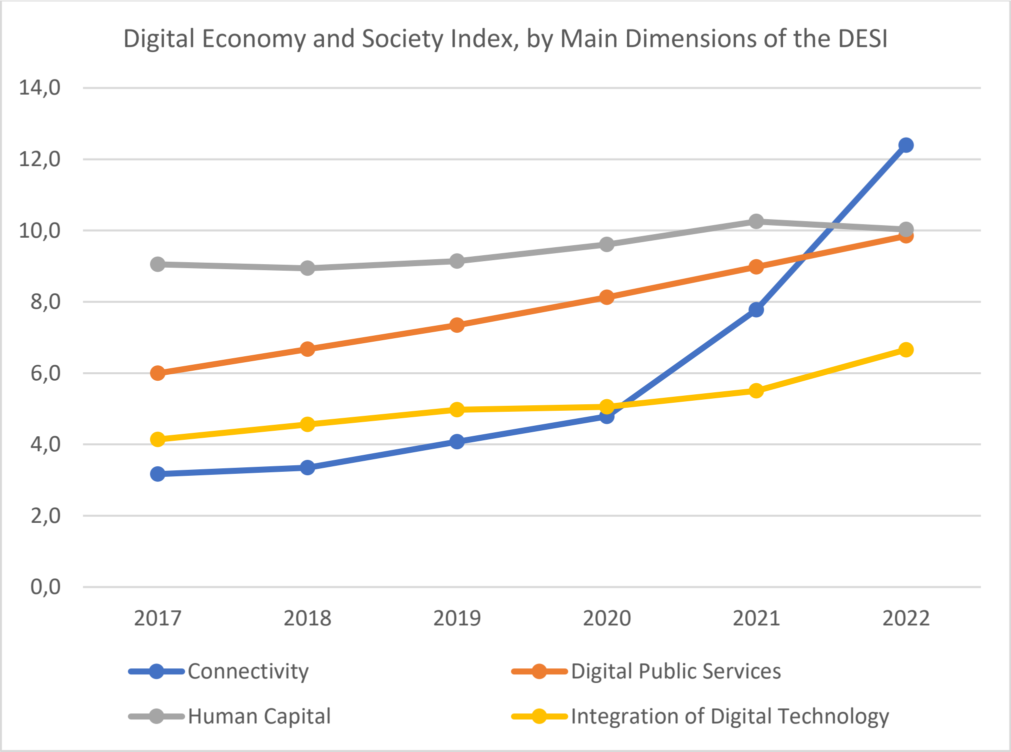
4.2.4 Greece

Greece is lagging significantly in digitalisation generally, even though recent progress has been documented, especially during and after the COVID-19 pandemic. In total, the country ranks 25th of 27 EU Member States in the DESI 2022, while the performance in the various sub-indexes varies. **In the human capital sub-dimension, Greece is three places higher than the total score (22nd), with 52% of individuals having basic digital skills** (54% of the EU average). Connectivity after 2020 has improved outstandingly in the country, but it still lags behind the EU, ranking 22nd. Especially, the share of households with at least 100 Mbps fixed broadband take-up is only 9%, while the EU average is 41%. In the integration of technology by businesses, Greece performs 22nd among the EU Member States with 39% of SMEs, the dominant firm type in the country, having at least a basic level of digital intensity (EU average is equal to 55%), though the share of SMEs selling online is slightly higher than the EU average, 20% and 18% respectively.

In digital public services, the country ranks almost last (26th), with the indicators of Digital public services for citizens (score of 52 out of 100) **and businesses** (score of 48 out of 100) **being significantly lower than the EU averages** (score of 75 and 83 accordingly). Greece performs better in the indicators of open data (82% of maximum score, EU average 81%) and in e-Government users with a share of 69% of internet users while on average, 65% of internet users in EU, use e-Government services.

Figure 23 Comparison of Greece's digital performance to EU in the DESI 2022





Source: European Commission, Digital Scoreboard

According to Statista, **the projected revenue in the Digital Health market could reach € 311.00 million in 2023** with an annual growth rate (CAGR 2023-2027) of 8.70%, leading to a projected market volume of € 434.20 million after five years. The top market segment is estimated to be eHealth (projected total revenue of € 172.80 million in 2023).

Greece does not yet have established a dedicated digital health policy, though, in June 2021, the Bible of Digital Transformation by the Digital Governance Ministry was published, which is the digital strategy of the country for the 2020-2025 period. The National Digital Strategy relies on seven Strategic Axes of Intervention a) Connectivity, b) Digital Skills, c) Digital Public Services, d) Digital Business, e) Digital Innovation, f) Advanced Technologies, and g) Integration of Technology in every sector of the economy. Chapter 9 describes the digital transformation of sectors of the Greek economy, and among them, the relative policy framework in the field of health is provided. Specifically, 26 actions for Digital Health are described in the strategy and also, to some extent, the secondary use of healthcare data is mentioned. Initiatives include the strengthening of health information security and managing citizen consent for access to their data, improving the quality, interoperability and access to health data and the expansion and development of Patient Registries[86]. **Greece has a number of health-data collection registries and agencies supporting the primary use of data**, as Shape 3 describes, that could potentially provide insights about the healthcare system and governance.

[86] Greek Government. (2021). Greece 2.0-national recovery and resilience plan.

The Recovery and Resilience Plan (RRP) of Greece allocates a significant part (more than € 2.7 billion) towards the digitalisation of public administration, where public health digitalisation is also included[87]. A **key investment in digital health and data usage is the “Planning Unification and support of the Operation of the Registries of HDIKA S.A. in the Field of Health and Social Security”** (budget of € 15.2). HDIKA S.A. offers a variety of services through an "ecosystem" of information systems, applications and electronic services in the fields of Health and Social Security. Those systems differ significantly because they have been developed across time for various or complementary objectives and, in many cases, using different techniques. To establish the necessary interoperability, both between internal and external systems, the investment project aims to plan, develop, integrate and support services in three basic information infrastructures of HDIKA a) the Electronic Prescribing System, b) the design and development of a Unified Register of HDIKA (EMI) and c) the design and development of a Central Interoperability Hub (API Gateway)[88]. Another important investment project through the National RRP is the “Digitalization of the Archives of the Public Health System” with a budget of € 190 million. The project's purpose is, through the digitalisation, normalization and matching procedures, to result in the availability of the patient file (electronic or physical), contributing to quality patient services. After completion, the provision of online services to end users regarding access to medical history will be possible.

[87] European Commission. (2022b). The digital economy & society index: Country profile of Greece

[88] HDIKA S.A.

Shape 3 Health-data collection registries and agencies supporting the primary use of data in Greece

Hellenic e-Government Center for Social Security (IDIKA)

- e-Prescription
- Individual Electronic Health Record
- Primary NHS and related data

Business Intelligence (BI) – Hellenic Ministry of Health

- Detailed data of the NHS
- NHS Data warehouse
- Operational utilization of data

GRNET

- Information systems infrastructure
- Health Data Centre
- National Blood Donor Registry

Hellenic National Organization for Health Care Services (EOPYY)

- e-DAPY – data collection for prescribed examinations
- Health service data for citizens and health sector professionals

Hellenic National Organization for Medicines (EOF)

- Medicinal products sales data
- Medicinal products quality data
- Archive of medicinal product approvals

Hellenic National Public Health Organization (EODY)

- Epidemiological data
- Statistical data on the surveillance of infectious diseases
- monitoring systems

Center for Documentation and Cost Estimation of Hospital Services (KETEKNI) – Hellenic DRG Institute

- Data on hospital expenses
- Data on the costing of hospital services

Hellenic Statistical Authority (ELSTAT)

- Population health data
- Data on the frequency of chronic diseases
- Data on the use of health services
- Data on behavioral factors that affect population health

Organization for Quality Assurance in Health (ODIPY) SA

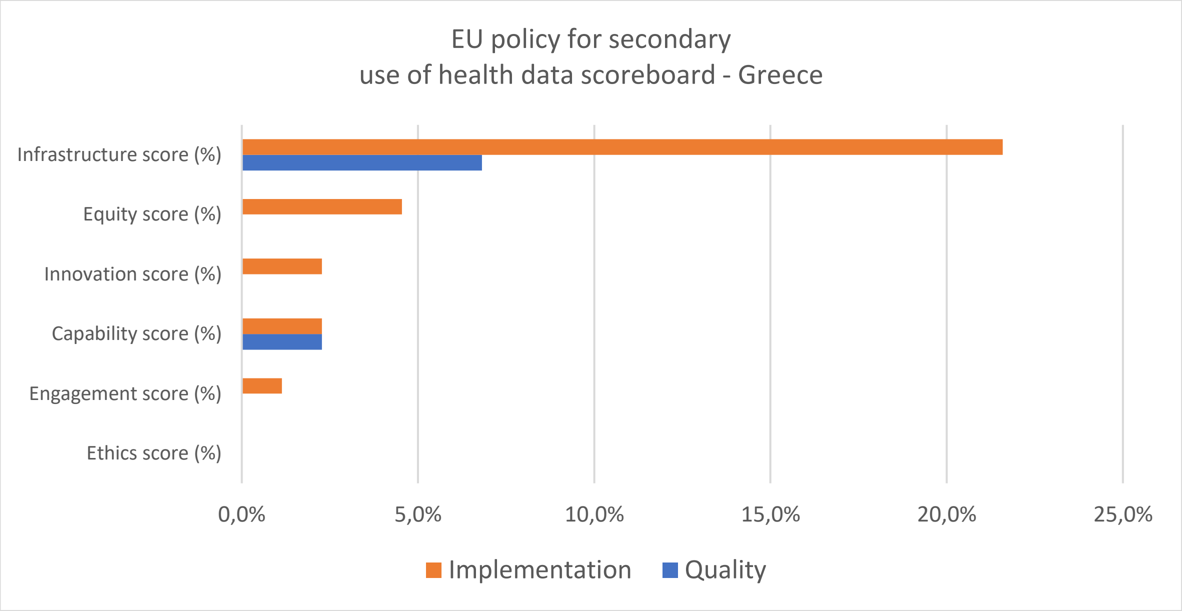
- Data on certified evaluation of health services
- Data on the quality of health services

Source: IOBE/FEIR

In Future Proofing Healthcare Index, **Greece ranks 26th in Europe and 30th in the dimension of health information**. In all sub-indexes of the health information index Greece lags behind, ranking 23rd in Cross-border transfer of Data securely, 30th in data infrastructure, and 17th in EHRs usage, but it should be mentioned that the country ranks 1st in the patient right to access data (source of data 2015). Also, in Telehealth, the country ranks 2nd and 13th in Patient portals. In the policy context, the country positions 29th with access to research data (taking into account open data policies and analysis of funders in the SHERPA-Juliet database) position the country 29th.
Regarding health information, the country ranks 16th and more specifically, Italy is 10th in the patient right to access data (source of data 2015), similar to the patient portals index (the year 2018). However, the country leads the way, ranking 3rd in the dimension of Cross-border transfer of Data securely (year of data 2018), while access to research is relatively low since the country ranks 16th. In Telehealth, Italy positions 17th (year of data 2015) and in the utilisation of EHRs 14th (data source 2015).

According to Boyd et al.[89]report, **the country performs better in the dimension of implementation and is significantly inferior regarding the quality of the policy regime**. Of the examined countries in this report, Greece is the only one listed as less prepared for the secondary use of health data. The country's policy framework and its implementation are less advanced than the examined countries, with seven other countries that were in the same category. One of the main policy challenges for Greece is the lack of clarity regarding the implementation strategy of health data usage[90].

Figure 24 Secondary use of health data policy, Score of Greece



Source: Boyd et. al. (2021)

[89] Boyd, M., Zimeta, M., Tennison, J., & Alassow, M. (2021). Secondary use of health data in Europe. Open Data Institute, Roche.
[90] Ibid.

Concluding remarks and policy recommendations

Economic dimension

The data economy has increasingly become a driver of competitiveness, underlined by its sizeable contribution to GDP and (high-paid) jobs.

Important statistical figures clearly show that, **in both terms of state of art and growth rate of the data economy, the EU is lagging behind the US and is being increasingly challenged by China**.

Within the EU, the development of the data economy differs greatly by country and size.

Northern EU countries are at the top of the ranking, showing a good "data ecosystem", with enterprises that perform particularly well in terms of data analysis and the use of enabling technologies such as cloud computing. On the other hand, **Southern (and Eastern) EU countries fall in the bottom half**, highlighting not only the need to invest in skills but also in the development of enabling technologies.

SMEs are often not equipped with an adequate set of skills to exploit the important opportunities that can arise from data analysis and are, perhaps, affected by a lack of awareness or understanding of the potential benefits of data analysis for their business. About one third of enterprises with over 250 employees perform Big Data analysis internally, while more than 10% outsource it to other companies or organizations vs. roughly 19% companies with 40 to 249 employees conducting internal analyses and only 5% relying on external analysis.

The **role of government** is instrumental in fostering the necessary underlying driving factors, regulating the market, but also providing access to its datasets.

More investment in R&I and a revision of educational and training programs should be pursued as a high priority.

In the first field, **distributed high performance computing infrastructure** should be built to create data lakes, shared repositories that can host any type of unstructured data, and make it accessible to analytics and machine learning tools put in place by any entity unable to develop their own data centers (such as SMEs, research and academic institutions, government agencies, non-profit organizations, etc). This will be achieved by improving existing computation centers and creating new ones, connecting them through a high-speed data transfer network.

Second, while basic training in digital skills is often included in educational programs, schools and training, specialist digital skills in emerging technologies is often lacking. As AI, blockchain and IoT and other technologies are gradually becoming more pervasive in our lives, **people need to update their skills fast, as well as the understanding of the opportunities and risks at stake**. This is also pivotal to fully taking advantage of new technologies and new business models and boosting the EU economic potential. Initiatives encouraging the development of a digital awareness and mindset for continuous upskilling could be useful to this end, to make citizens and employees more willing to embrace new technologies. **Digital skills and the understanding of emerging technologies should not be limited to ICT specialists, but also open to a wider population that could apply them in different fields**.

SMEs should be reached by Digital Innovation Hubs and other public and private centers supplying training but also business and technology advice and other services.

Specifically, EU policies should target reducing the disparities within the continent using a mix of European and national funds. The **Resilience and Recovery Facility**, providing important financial resources and reform requirements for EU Member States (especially the Southern), **is a great opportunity to accelerate this convergence and should not be wasted**.

Geopolitical dimension

Data is one of the most valuable resources in today’s global competition – but it is not yet seen as a global common that leads to collaboration. So far, global data flows are still governed through a maze of multilateral, bilateral, unilateral, and ad hoc rules, principles, and voluntary frameworks that are not always accepted or applied by all actors. **Cross-border international collaboration** on this issue is far limited, with ups and downs in the success of a common global agenda on data governance. Also, **data governance** is getting balkanized in blocs that propose different, if not contrasting, data models. Doing so is as important as strategic for the maintenance of an international security and peace order which growingly relies on the power over data and has strong impacts on three layers: security, economic, and rights.

It is by no chance that the EU has been addressing how their goods, services, assets, and personal data relate to third countries through several ways: **regulation, the role of multilateral initiatives, “coalitions of the willing” and international meetings, and the building-up of digital diplomacy**.

Still, the EU faces **several challenges** that should be tackled to complete a comprehensive strategy on the geopolitics of data. First, the main challenge for the EU to deploy this regulatory tool as a geopolitical asset relies on whether the EU will get to **influence other countries** to follow the same approach. It is not only about imposing certain rules to those that already do interact with the EU, but about encouraging others to do the same with their owns.

Similarly, it is important to understand that **geopolitical strategies** should vary depending on the country and type of technology company, as firms may have different geopolitical approaches.

Third, it remains difficult to govern data internationally because how to define **Intellectual Property** in data is not straightforward. This is an issue that the European Union institutions are working on through the Data Act, especially in terms of defense-related data and data from sensitive, critical sectors.

Also, from the perspective of economic security, data governance should always be effectively aligned with the **export control regimes** currently agreed at the EU level, especially considering that the interpretation and implementation of this criteria is carried out at the national level.

Likewise, **the EU has an opportunity to partner with like-minded countries** as Japan and engage closely with the Indo-Pacific region through partners that have a clear vision on global technology governance but are not too explicitly aggressive towards China.

In this line, it will be important not to forget how to partner with developing countries or, particularly, digitally non-aligned countries. Also, **all digital diplomacy branches should pay**

attention to certain technologies that are still underdeveloped, not too marketized or not in place, but that could generate major competition across countries, such as the **metaverse**, which has been labelled as national security threat by China.

The European Union is developing an increasing package to address the governance of data globally speaking. To do so effectively, it will need to face a number of challenges -from the perspectives of security, economy, and rights- that are not always framed under the existing policies. **New scope, intensities, stakeholders’ engagement and a higher level of ambition and monitoring will be the drivers to make the EU’s leverage of its Data Strategy worldwide successfully with partners**.

Data Governance Act & Data Act

The 2020 EU Data Strategy Communication states the outlines of a future EU data economy. These outlines are reflected in posterior regulatory acts such as the **Data Governance Act (DGA)** and the **Data Act (DA)**.

The main idea is to create a data-driven economy with EU citizens at its centre. For this, the EU incentivizes all the actors, from public authorities to businesses, to share their data. **Through the DGA and the DA, the Commission seeks to construct a navigable data landscape, where users can easily control their data and give their consent for its use and reuse, while protecting confidential data, intellectual property rights and trade secrets.** This landscape is expected to fuel innovation, prevent power imbalances favouring gatekeeper companies, and boost competitiveness through the protection of SMEs. It aims to be a place where no competitive advantage results from owning property rights over data or data concentration, but instead from the transformation and combination of that data in order to produce added value.

On one hand, **most of the benefits of the EU Data Strategy are connected to more transparency, innovation, interoperability, better quality services, and fewer market barriers.** These are especially important if we consider that one of the main ambitions of the Commission is for the EU to “become a leading role model for a society empowered by data to make better decisions – in business and the public sector”. Using the conclusions of previous studies, we can say that the economic benefits envisioned in this Strategy would be significant and will be crucial in the EU’s positioning in the international economy.

On the other hand, **there are some motives for concern**. First, what is not addressed in the legal framework is the continuing **lack of incentives for competitors share their data**. What drives competitive businesses to altruistically give away their data to competitors? What prevents companies from freeriding? Furthermore, it is unclear whether **overall incentives for research and development** will be strengthened, given the mix of incentives caused by giving away and receiving data.

Second, the legal framework taken together determines a multitude of competent authorities with different levels of supervisory power. We point out that the **threat of insufficient or burdensome regulatory control and monitoring capacity** by these bodies may be a problem and delay the process.

Also connected to the functioning of these bodies is the **problem of coordination between Member States**, e.g., with respect to the choice of agencies and applicable penalties. Will there again be regulatory competition as happened under the GDPR? Furthermore, several dispositions delegate to every actor the responsibility to protect their data, which may result in **possible leaks of personal data** if we consider the different levels of capacity of each actor to guarantee this protection. Also, even though SMEs are protected in many forms, the **costs of compliance for businesses** will be a setback, namely because while this will mean added financial costs to some, it may also mean a total redesigning of the company's business model for others.

Although we expect the EU Data Strategy to have an overall positive impact, the **remaining uncertainty regarding its associated acts and their practical implementation** still needs to be addressed in the trilogue and will require further action through future legislative initiatives and industry-wide coordination activities.

European Health Data Space

The **European Health Data Space (EHDS)** planning could enhance the citizens digital access to their private health information, support access of medical professionals to health data, assist academia, regulatory activity and policy making by providing non-identifiable health data while facilitating complete adherence to the strict data privacy standards set by the EU

A **variety of benefits is expected since improved access and transfer of health data** in the healthcare sector could save 5.5 billion € for the EU over ten years in combination with € 5.4 billion that could be saved for the EU from optimal use of health data by the research and innovation community and also by the policymakers. Furthermore, the potential growth of digital health care is estimated between 20-30%. Another critical benefit is the boost of investments in Research and Development (R&D) by facilitating access to Real World Evidence.

Though the benefits of the EHDS could be significant for healthcare policy and innovation, certain **challenges** also emerge. **Health information is the most sensitive type of data, and privacy ensuring should always be a top priority**. Medical records contain sensitive information about patients, such as their medical history, diagnosis, and treatment. Therefore, **cybersecurity, storage and connection with other information** are issues of great concern since the EHDS requires interoperability among many different data sources. **Unidentified provision of data for research and other policy issues** should also be a critical aspect to ensure. Furthermore, **getting patients' permission to use their health data in a secondary way can be difficult** because they may worry about how their information will be used and who will have access to it.

Countries face a variety of challenges to overcome**. Fragmentation of the different data registries and their storage** is evident in the examined four countries. **Lack of standardization in collection of health data since systems**, terminology among the various registries differ hindering harmonisation and effective comparisons. Additionally, the quality of the analysis may be impacted by the fact that the **data may not always be comprehensive or reliable**. There is a lot of room for improvement with respect to enhance quality standards and validation procedures.

There is a **need to for a unified roadmap** for the proper utilization of data that could support transformation/rationalization of health care, health spending and the promotion of clinical research and innovation**. Establishing precise rules and policies for data security and privacy** in the healthcare industry is imperative. **Encouraging standardisation procedures**, which could entail the adoption of standard terminology and processes by various healthcare stakeholders, could also be useful. **Effective quality assurance mechanisms** could contribute significantly to the task. **Transparency in data management, privacy protection and taking patient consent** could increase trust and foster health digitalisation. Last, but not least, **fostering cooperation and collaborations** amongst various healthcare stakeholders could significantly promote the digitalisation of healthcare and the successful secondary data usage.